PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-341266
(43)Date of publication of application : 08.12.2000

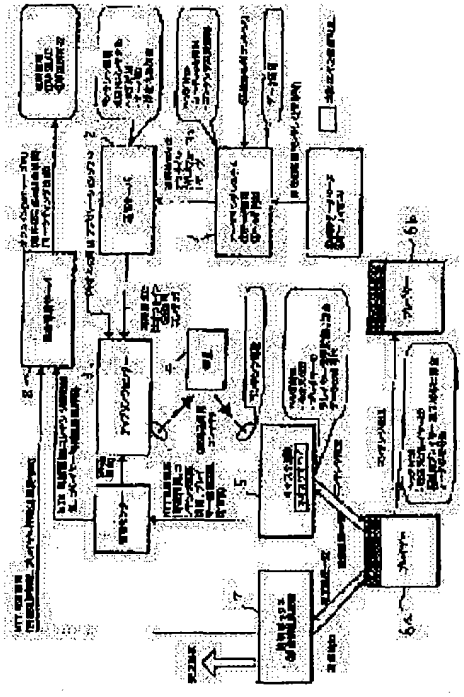
(51)Int.Cl. H04L 9/14
G06F 12/00
G06F 12/14
G06F 15/00
G09C 1/00
G10L 19/02
G10L 19/00
G10L 11/00
H04L 9/20
H04N 7/167

(21)Application number : 11-152208
(22)Date of filing : 31.05.1999

(71)Applicant : VICTOR CO OF JAPAN LTD
(72)Inventor : TANAKA YOSHIAKI
OKABE YASUHISA

(54) DATA TRANSFER METHOD, DATA TRANSFER METHOD IN CONTENTS SALES SYSTEM UTILIZING THE METHOD AND RECORDING MEDIUM RECORDING DATA

(57)Abstract:
PROBLEM TO BE SOLVED: To prevent reproduction of real data from being hindered while preventing copying in a sales system for contents data such as music data.
SOLUTION: The contents sales system is a system where host serves contents data such a music and transfers (downloads) them to user side players 6a, 6b via a KIOSK installed terminal 5 and a network such as the Internet. A different encryption system is adopted for contents data requiring reproduction in an early timing from that for header information requiring no early timing, the encryption system not taking much time for decoding is adopted for the contents data and a complicated encryption system taking much time for decoding is adopted for the header information storing reproduction key information or the like.



使用後返却願います

(2)

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2000－341266
(P2000－341266A)
(43)公開日　平成12年12月8日(2000.12.8)

(51)Int.Cl.'		識別記号	FI		テーマコード'(参考)
H04L	9/14		H04L	9/00	641　5B017
G06F	12/00	545	G06F	12/00	545M　5B082
	12/14	320		12/14	320B　5B085
	15/00	330		15/00	330Z　5C064
G09C	1/00	610	G09C	1/00	610B　5D045

審査請求　未請求　請求項の数3　ＯＬ　（全 30 頁）　最終頁に続く

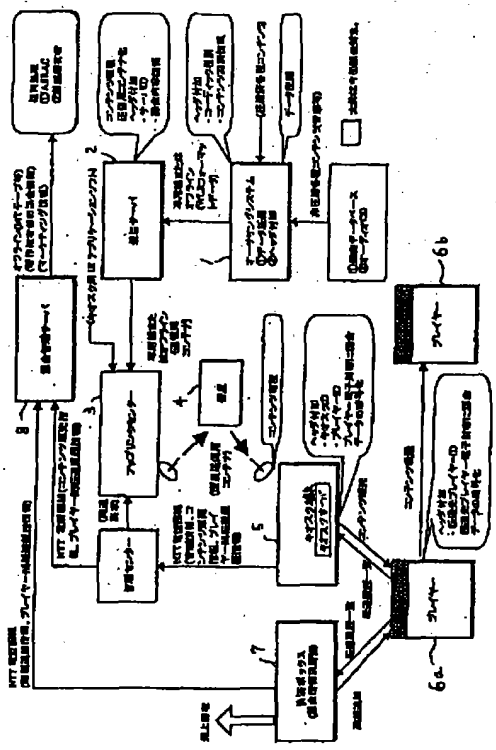
(21)出願番号　特願平11－152208
(22)出願日　平成11年5月31日(1999.5.31)

(71)出願人　000004329
日本ビクター株式会社
神奈川県横浜市神奈川区守屋町３丁目12番地
(72)発明者　田中　美昭
神奈川県横浜市神奈川区守屋町３丁目12番地　日本ビクター株式会社内
(72)発明者　岡部　恭尚
神奈川県横浜市神奈川区守屋町３丁目12番地　日本ビクター株式会社内

最終頁に続く

(54)【発明の名称】　データの転送方法、その方法を利用したコンテンツ販売システムのデータ転送方法及びそのデータが記録された記録媒体

(57)【要約】
【課題】　音楽データのようなコンテンツデータの販売システムにおいて、コピー防止を図りつつ、実データの再生に支障をきたすようなことがないようにする。
【解決手段】　音楽などのコンテンツデータをホストが提供してキオスク置端末５やインターネットなどのネットワークを介してユーザ側のプレーヤ６ａ，６ｂに対して転送（ダウンロード）するコンテンツ販売システムであり、早いタイミングでの再生が要求されるコンテンツデータと、そこまでの要求がないヘッダ情報との暗号化方式を異ならせ、コンテンツデータの方を復号化に時間を要しない暗号化方式にし、再生鍵情報等が格納されるヘッダ情報の方を復号化に時間を要する複雑な暗号化方式にする。



【特許請求の範囲】
【請求項１】転送元端末から転送先端末に対して、そのデータ再生時の処理速度が所定の速度で要求される第１のデータと、それより遅い処理速度の再生が許される第２のデータとを含んで転送するデータの転送方法において、
前記第１のデータを所定の第１の再生鍵を用いて暗号化すると共に、前記第２のデータを前記第１の再生鍵を用いて暗号化して復号化するときの処理速度より復号化に時間を要する第２の再生鍵を用いて暗号化し、これら暗号化された第１と第２のデータを転送するようにしたことを特徴とするデータの転送方法。
【請求項２】前記データの転送方法は、販売元端末より販売先端末にコンテンツデータを配信するコンテンツ販売システムのデータ転送方法であり、
前記第１のデータは、少なくとも実データであるコンテンツデータであり、前記第２のデータは少なくとも前記コンテンツデータに付加されるヘッダ情報であり、前記第１の再生鍵による暗号化は、所定バイト数の乱数で生成された前記第１の再生鍵と前記コンテンツデータとをＸＯＲ演算により暗号化し、前記２の再生鍵による暗号化は、所定バイトの乱数で生成された第２の再生鍵により前記第２のデータがＤＥＳ暗号化されたものであることを特徴とするコンテンツ販売システムのデータ転送方法。
【請求項３】請求項１又は２記載の転送方法により転送されたデータを所定の領域に記録したことを特徴とする記録媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、音楽などのコンテンツデータをホストが提供して販売店設置端末やインターネットなどのネットワークを介してユーザ側のプレーヤに対して転送（ダウンロード）するデータの転送方法、その方法を利用したコンテンツ販売システムのデータ転送方法及びそのデータが記録された記録媒体に関する。
【０００２】
【従来の技術】近年、音楽などのコンテンツデータ（ソフト）をユーザ側に販売するシステムとして、ＣＤ（コンパクト・ディスク）やＤＶＤ（デジタル・バーサタイル・ディスク）などの有料の記録媒体を用いる代わりに、対価の支払いを条件として販売店設置端末やインターネットなどのネットワークを介してユーザ側のプレーヤ内のハードディスクや半導体メモリなどの記録媒体に転送してこれを再生するコンテンツ販売システムあるいはネットワーク配信システムが着目されている。
【０００３】コンテンツ販売システムの一例としては、コンテンツデータをホスト側から衛星通信回線や公衆電話回線を介して販売店設置端末に転送し、更に販売店設置端末からプレーヤに転送する販売店設置端末経由方式が考えられる。他の経由方式としては、コンテンツデータをインターネット・サーバ（ホスト）側からインターネット及びインターネットクライアント（ユーザパソコン）を介してプレーヤに転送するインターネット経由方式が考えられる。
【０００４】
【発明が解決しようとする課題】ところで、このようなコンテンツ販売システムでは、不正にコンテンツデータがコピーされないように送信側のＩＤ（識別情報）や受信側のＩＤに基づいて暗号化してから送信するようなことが考えられている。ところが、そのように暗号化しても、何らかの手法によりＩＤが知られ、そのＩＤを用いて暗号を解読して不正なコピーが行われることが懸念されている。そこで、本発明では、このような問題に鑑みて不正なコピーが行われないような暗号化を行うと共に、より速い再生速度での再生が要求される例えば実データであるコンテンツデータと、それほど速い処理速度での再生が要求されない例えばヘッダ情報等との暗号化方式を異ならせ、コンテンツデータの方は時間を要せずに復号化できる暗号化方式とし、ヘッダ情報の方は復号化に多少時間を要しても暗号がもれないような複雑な暗号化方式とすることで、再生鍵データが含まれる情報部を今まで以上に知られにくくすると共に、再生タイミングに支障をきたすようなことがないようにしようというものである。
【０００５】
【課題を解決するための手段】本発明は、上記課題を解決するために、以下の１）～３）の手段より成る。すなわち、
１）転送元端末から転送先端末に対して、そのデータ再生時の処理速度が所定の速度で要求される第１のデータと、それより遅い処理速度の再生が許される第２のデータとを含んで転送するデータの転送方法において、前記第１のデータを所定の第１の再生鍵を用いて暗号化すると共に、前記第２のデータを前記第１の再生鍵を用いて暗号化して復号化するときの処理速度より復号化に時間を要する第２の再生鍵を用いて暗号化し、これら暗号化された第１と第２のデータを転送するようにしたことを特徴とするデータの転送方法。
２）前記データの転送方法は、販売元端末より販売先端末にコンテンツデータを配信するコンテンツ販売システムのデータ転送方法であり、前記第１のデータは、少なくとも実データであるコンテンツデータであり、前記第２のデータは少なくとも前記コンテンツデータに付加されるヘッダ情報であり、前記第１の再生鍵による暗号化は、所定バイト数の乱数で生成された前記第１の再生鍵と前記コンテンツデータとをＸＯＲ演算により暗号化し、前記２の再生鍵による暗号化は、所定バイトの乱数で生成された第２の再生鍵により前記第２のデータがＤ

ＥＳ暗号化されたものであることを特徴とするコンテンツ販売システムのデータ転送方法。

３）請求項１又は２記載の転送方法により転送されたデータを所定の領域に記録したことを特徴とする記録媒体。

【０００６】

【発明の実施の形態】以下、図面を参照して本発明の実施の形態を説明する。図１は本発明が採用される販売店端末（キオスク端末）を経由するコンテンツ販売システムの一例を示す構成図、図２は図１のプレーヤに配信される販売ヘッダの構成を示す説明図、図３は図１のオーサリングシステムにより付与される販売ヘッダの構成を示す説明図、図４は図１のプレーヤに販売サブヘッダの構成を示す説明図である。

【０００７】図１はコンテンツ販売システムの一例として、ＪＲの売店（以下、キオスク）に販売店端末（以下、キオスク端末）５を設置した販売店設置端末経由方式のシステムを示している。まず、ホスト側では非圧縮の音楽コンテンツをオーサリングシステム１により例えばTwin VQ方式で圧縮し、次いでこの圧縮データを詳細の後述する再生鍵データで暗号化する。また、オーサリングシステム１ではこの再生鍵データを１次暗号化してこの１次暗号化再生鍵データと暗号化コンテンツを所定のデータ構造として記録し送信サーバ２、アップリンクセンタ３、衛星４を介してキオスク端末５のサーバに転送する。なお、この販売店設置端末経由方式のシステムでは、コンテンツを衛星４を介してキオスク端末５へ供給する代わりに、別の又は過渡的な供給方法として、記録済サーバを物流により定期的に交換するようにしてもよく、これに限られるものではない。さらに、販売店設置端末はキオスクの他、コンビニエンス・ストアなどの他の販売店に設置するようにしても良い。

【０００８】キオスク端末５は、１次暗号化再生鍵データを２次暗号化してこの２次暗号化再生鍵データと暗号化コンテンツをプレーヤ（図中プレイヤーと示すこともある）６ａにダウンロードする。このとき、キオスク端末５とプレーヤ６ａの間はＩＥＥＥ１３９４インタフェースを介して接続され、プレーヤ６ａはダウンロード前にあらかじめ自己のＩＤをキオスク端末５に転送する。また、コピー元プレーヤ６ａとコピー先プレーヤ６ｂ間では、２次暗号化再生鍵データと暗号化コンテンツが再転送可能であり、この場合にもコピー先プレーヤ６ｂは再転送前にあらかじめ自己のＩＤをコピー元プレーヤ６ａに転送する。このシステムの課金方式では、ユーザがプリペイド方式で電子チケットを購入することにより残高がプレーヤ６ａ内の電子財布に記憶され、また、課金情報がプレーヤ６ａから決済ボックス７を介して課金管理サーバ８に転送される。この課金管理サーバ８は、キオスク端末５や後述のＷｅｂサーバ９を通じて前記の課金情報や各プレーヤ６ａ，６ｂの転送履歴を回収して、これらの情報をもとに著作権管理等を行うようにしている。

【０００９】また、この販売システムは、前述のキオスク端末を経由するシステムであると共に、インターネット方式により販売する経路も有している。図２は、そのインターネット方式による販売システムを示す図である。まず、ホスト側では販売店設置端末経由方式と同様に、非圧縮の音楽コンテンツをオーサリングシステム１により例えばTwin VQ方式で圧縮し、次いでこの圧縮データを再生鍵データで暗号化する。また、オーサリングシステム１ではこの再生鍵データを１次暗号化してこの１次暗号化再生鍵データと暗号化コンテンツを所定のデータ構造として記録し送信サーバ２、Ｗｅｂサーバ（インターネットサービス用サーバ）９に転送する。

【００１０】Ｗｅｂサーバ９は１次暗号化再生鍵データを２次暗号化して２次暗号化再生鍵データと暗号化コンテンツをインターネットサービス用ＰＣクライアント１０（ＰＣクライアントともいう）を介してプレーヤ６ａにダウンロードする。このとき、Ｗｅｂサーバ９とＰＣクライアント１０の間がダイヤルアップ接続により接続されるとともに、ＰＣクライアント１０とプレーヤ６ａの間がＩＥＥＥ１３９４インタフェースを介して接続され、また、プレーヤ６ａはダウンロード前にあらかじめ自己の端末ＩＤをＰＣクライアント１０を介してＷｅｂサーバ９に転送する。また、同様に、コピー元プレーヤ６ａとコピー先プレーヤ６ｂ間で２次暗号化再生鍵データと暗号化コンテンツが再転送可能であり、この場合にもコピー先プレーヤ６ｂは再転送前にあらかじめ自己のＩＤをコピー元プレーヤ６ａに転送する。また、ユーザがプリペイド方式で電子チケットを購入することにより残高がプレーヤ６ａ内の電子財布に記憶され、課金情報がプレーヤ６ａからＰＣクライアント１０、Ｗｅｂサーバ９を介して課金管理サーバ８に転送される。

【００１１】プレーヤ６ａ、６ｂに転送されるフォーマットは、販売店設置端末経由のシステムとインターネット経由のシステムにおいて共通であって、販売コンテンツ毎に販売ヘッダと、販売サブヘッダと暗号化コンテンツデータを含み、販売サブヘッダは販売コンテンツ内の曲目数Ｎ毎に付与される。暗号化コンテンツデータはコンテンツヘッダ、サウンドストリーム（音楽コンテンツ）、テキストデータ（曲名、アーティスト名など）、拡張データなどを含む。

【００１２】販売ヘッダは図３に示すように、販売コンテンツ内の曲目数Ｎに応じて可変長（＝６４Ｎ＋Ｍバイト（Bytes））であって、

・１バイトの販売ヘッダバージョンと、
・１バイトの販売ヘッダサイズと、
・１バイトの保留（Reserved）データと、
・１バイトの転送制御データと、
・８バイトのコンテンツ販売ＩＤと、

・８バイトの転送元ＩＤと、
・２バイトの販売チケット数と、
・１バイトの販売サブヘッダ数と、
・１バイトのコンテンツ曲数と、
・３２バイトの制作タイトル名と、
・１６バイトの制作会社名と、
・４×Ｎバイトの曲目毎のデータ長と、
・８×Ｎバイトの曲目毎の曲名と、
・８×Ｎバイトの曲目毎のアーティスト名と、
・４×Ｎバイトの曲目毎の演奏時間と、
・Ｋバイト（６４Ｎ＋Ｍ－Ｋバイト目～６４Ｎ＋Ｍバイト目）の再生鍵データ（暗号化データ）を含む。

【００１３】これに対し、図４はオーサリングシステム１によりマスタリング時に付与される販売ヘッダの構成を示し、この販売ヘッダは図２に示すデータの他に、制作タイトル名、Ｎ曲分の曲名、Ｎ曲分のアーティスト名、Ｎ曲分のＩＳＲＣ（International Standard Recording Code）を含む。

【００１４】販売サブヘッダは図５に詳しく示すように、
・１バイトのサブヘッダバージョンと、
・１バイトのサブヘッダサイズと、
・１バイトの保留（Reserved）データと、
・１バイトの転送制御データと、
・８バイトのコンテンツ販売ＩＤと、
・８バイトの転送元ＩＤと、
・２バイトの販売チケット数と、
・１バイトの指定曲番と、
・３２バイトの制作タイトル名と、
を含む。

【００１５】前記の販売ヘッダ及び販売サブヘッダ内の転送制御データは図６に詳しく示すように、４ビットｂ０～ｂ３の再転送世代数データと４ビットｂ４～ｂ７の再転送禁止／許可データを含む。
・再転送世代数ビットｂ０～ｂ３
００００：再転送禁止
０００１～１１１１：再転送世代数（再転送許可）著作権者（ホスト）側が設定して再転送毎にカウントダウンし、００００で再転送禁止
・再転送禁止／許可ビットｂ４～ｂ７
０００：再転送許可
０００１：再転送禁止
００１０～１１１１：保留（Reserved）

【００１６】また、前述のオーサリングシステム１における暗号化処理は次のように行われる。図７は、その処理を説明するためのフローチャートである。まず、販売ヘッダ毎に所定バイトの再生鍵データを乱数で作成し（ステップＳ１）、次いで販売コンテンツデータをコンテンツヘッダ、サウンドストリーム（音楽コンテンツ）、テキストデータ（曲名、アーティスト名など）、拡張データの各領域毎に分けて、上記の再生鍵データ（乱数）と所定バイトずつに排他的論理和（ＸＯＲ）演算することにより、販売コンテンツデータを各領域毎に独立して暗号化する（ステップＳ２）。

【００１７】また、（販売ヘッダの指定項目順の文字列）＋（販売サブヘッダの指定項目順の文字列）の合成文字列に基づいてハッシュ関数（ＭＤ５）により所定バイトのハッシュ値を作成し（ステップＳ３）、次いで上記の再生鍵データとハッシュ値をＸＯＲ演算することにより１次暗号化再生鍵データを作成する（ステップＳ４）。そして、１次暗号化再生鍵データを販売ヘッダの再生鍵データ領域に格納して暗号化コンテンツとともに販売元端末（キオスク端末５、Ｗｅｂサーバ９）に伝送する（ステップＳ５）。このように、ステップＳ３とＳ４により販売ヘッダに基づく情報により再生鍵データを暗号化することにより販売ヘッダとコンテンツデータの組み合わせを改ざんした場合には復号できないようにしている。

【００１８】また、図８は販売元端末（キオスク端末５、Ｗｅｂサーバ９）の再生鍵の２次暗号化の処理フローを示し、まず、１次暗号化再生鍵データを転送先プレーヤＩＤを鍵としてＤＥＳ暗号化して転送先プレーヤ６ａの２次暗号化再生鍵データを作成し（ステップＳ１１）、次いでこの２次暗号化再生鍵データを暗号化コンテンツとともに販売先端末（プレーヤ６ａ）に伝送する処理となっている（ステップＳ１２）。

【００１９】また、図９は販売先端末（転送先プレーヤ６ａ）の暗号化された再生鍵及びコンテンツデータの復号処理方法の処理フローを示している。まず、２次暗号化再生鍵データを自己のプレーヤＩＤを鍵としてＤＥＳ復号することにより１次暗号化再生鍵データに復号するとともに（ステップＳ２１）、（販売ヘッダの指定項目順の文字列）＋（販売サブヘッダの指定項目順の文字列）の合成文字列に基づいてハッシュ関数（ＭＤ５）により所定バイトのハッシュ値を作成する（ステップＳ２２）。次いでこれらの１次暗号化再生鍵データとハッシュ値をＸＯＲ演算することにより元の再生鍵データに復号し（ステップＳ２３）、次いで暗号化販売コンテンツデータを所定バイトずつ元の再生鍵データとＸＯＲ演算することにより元の販売コンテンツデータに復号し、これを伸長して再生する（ステップＳ２４）。

【００２０】特に、本システムの暗号化方式では、コンテンツデータやテキストデータなどの実データをＸＯＲ演算で暗号化し、ヘッダ等の実データと異なるデータはＤＥＳ暗号化方式で暗号化している。これは、再生時の処理速度に対応しているもので、再生時に処理速度が速く要求される実データは復合化のことを考慮して複合化が速く行えるＸＯＲ暗号化方式を採用し、それほどの処理速度が要求されないヘッダ情報には、それより復号化に時間を要する複雑なＤＥＳ暗号化方式として、再生速

度とデータの流出との両方を考慮した暗号化としている。

【００２１】また、前記のプレーヤ６ａ，６ｂは、図１０に示す構成で、プレーヤ６ａの符号のみを用いて説明する。プレーヤ６ａは、データ転送インターフェース６ａ-1、電子財布部６ａ-2、表示部６ａ-3、操作部６ａ-4、記憶部６ａ-5、暗号化／復号化部６ａ-6、データ圧縮／伸長部６ａ-7、再生部６ａ-8、出力端子６ａ-9、制御部6a-10及び内部バス６ａ-11から構成されている。

【００２２】データ転送インターフェース６ａ-1は、送信側プレーヤと受信側プレーヤとの間、これらプレーヤとキオスク端末５との間、又は、後述のＰＣクライアント（パソコン）とのデータ転送に使用される。電子財布部６ａ-2は、電子マネーの受け取り、支払いをすることができる。プリペイド方式により電子マネーを予めデポジットしておき、その電子マネーをコンテンツ料金に応じて減額するようにしている。後述の説明では、プリペイド方式による説明としているが、周知のクレジット方式としても良い。

【００２３】表示部６ａ-3は、電子財布の電子マネーの残額や、端末間のデータ送受信時の送受信状況、コンテンツ再生時の再生状況、コピーの可否等を表示する。操作部６ａ-4は、複数のデータの中から再生したいデータを探し出すためのデータ頭出し操作、再生時の再生音量操作等に使用される。記憶部６ａ-5には、キオスク端末５から受け取ったヘッダ情報やコンテンツデータや再生、他の携帯端末等から受け取ったヘッダ情報やコンテンツデータ等が記憶される。

【００２４】暗号化／復号化部６ａ-6は、認証データの生成やコンテンツデータ、再生鍵及びヘッダ情報の暗号化又は復号化を行う。データ圧縮／伸長部６ａ-7は、データを圧縮、又は圧縮されているデータを伸長する。転送されるデータは、転送効率を上げるため圧縮状態とする。従って、データ送信前にデータを圧縮し、データ受信後に必要に応じて圧縮データを伸長する。再生部６ａ-8は、コンテンツデータから音声、テキストデータ等を再生する。再生された音声等は、出力端子６ａ-9から外部に出力される。制御部６ａ-10は、上記各部の制御や、履歴転送回数、コンテンツ販売ＩＤ、転送元ＩＤ及び転送制御データの履歴数分の登録等を内部の記憶部mに行わせる。

【００２５】次に、各端末間の処理手順につき順次詳述していく。まず、図１１、図１２はキオスク端末（ホスト側）５とプレーヤの間の転送手順を示している。図５においてキオスク端末５と例えば上記構成のプレーヤ６ａがＩＥＥＥ１３９４インタフェースを介して接続された状態である。また、図１１以下の図中、「Form 1」、「Form２」…などは信号フォーマットの番号を示すもので、詳細な説明は省略するが、前述の販売店設置端末経由のシステムとインターネット経由のシステムにおいて共通であって、基本的には図１３に示すように、発信元コード（図１４に示すシステム構成装置の種類を示すコード）と、コマンドコード（図１５、図１６参照）と、データ長と実データ（暗号化データ）により構成されている。ただし、転送元（キオスク端末５、Ｗｅｂサーバ９）からプレーヤ６ａに送信される各種の「要求」や、プレーヤ６ａから転送元５、９に送信される各種の「通知」のフォーマットは、実データは含まれず、発信元コードと、コマンドコードと、データ長（＝オール０）のみにより構成されている。

【００２６】キオスク端末５内において、このキオスク端末５内には図示はしていないが、データ転送インターフェース、表示部、記憶部、暗号化／復号化部、再生部、出力端子、制御部、内部バスなど、プレーヤ６ａ，６ｂとほぼ同様の機能部が含まれている。まず、図示しない暗号化部において例えば８バイトの乱数認証データＤ１を作成し、決済ボックス、キオスク端末、各プレーヤ、Ｗｅｂサーバ９及びＰＣクライアント１０において共通に保持している共通鍵K1～K6の一つである共通鍵データＫ１によりＤＥＳ暗号化し、この暗号化された認証Ａデータを８バイトの所定の送信フォーム「１」（図中「Form　１」と示される）のプレーヤ認証ＡデータＤ１としてデータ転送インターフェース介してプレーヤ６ａに送信する。

【００２７】プレーヤ６ａでは、このプレーヤ認証ＡデータＤ１をデータ転送インターフェース６ａ-1を介して受信し、暗号化／復号化部６ａ-6において、共通鍵データＫ１によりＤＥＳ復号化し、この復号化で得られた認証ＡデータＤ１を他の共通鍵データＫ２によりＤＥＳ暗号化し、返信プレーヤ認証Ａデータを作成する。それと同時に、８バイトの乱数認証ＡデータＤ３を作成し、この認証ＡデータＤ３を他の共通鍵データＫ３によりＤＥＳ暗号化し、このデータをホスト認証Ａデータとし、所定の送信フォーム「２」でホスト認証Ａデータと前記返信プレーヤ認証ＡデータとをＷびキオスク端末５に返信する。

【００２８】キオスク端末５では、データ転送インターフェースを介して返信プレーヤ認証Ａデータとホスト認証Ａデータとを受信し、これらを暗号化／復号化部に供給し、ここで、返信プレーヤ認証Ａデータを共通鍵データＫ３によりＤＥＳ復号化し、この復号化された認証ＡデータＤ１と送信認証ＡデータＤ１とが制御部において照合される。照合の結果、不一致の場合には、このキオスク端末５側において行った前述の処理を２回まで再度実行する。それでも不一致する場合にはキオスク端末５における処理を中止する。

【００２９】また、一方、一致の場合には、受信ホスト認証Ａデータを共通鍵データＫ３によりＤＥＳ復号化し、この復号化で得られた認証ＡデータＤ２を、他の共通鍵データＫ４によりＤＥＳ暗号化し、返信ホスト認証

Aデータとし、このデータを所定のフォーム「3」でプレーヤ６ａに送信する。プレーヤ６ａの暗号化／復号化部６ａ-6では、この返信ホスト認証Aデータを共通鍵データ４によりＤＥＳ復号化し、復号化された認証AデータＤ２を得て、この復号化された認証AデータＤ２と送信ホスト認証Aデータとを制御部６ａ-10において照合し、一致の場合には所定の送信フォーム「4」でホスト認証をキオスク端末５に送信し、その後の処理を受け付ける。また、一方、認証不一致の場合には、フォーム「4」の認証不可をキオスク端末５に送信し、これ以降の処理の受付を禁止する。

【００３０】次に、キオスク端末５からプレーヤ６ａに対し、所定の送信フォーム「5」のプレーヤＩＤの送信要求がなされる。これを受信したプレーヤ６ｂ側では暗号化／復号化部６ａ-7において、自己プレーヤＩＤをホスト認証に使用した認証AデータＤ２を鍵として１６バイトづつＤＥＳ暗号化し、このデータを所定の送信フォーム「6」でキオスク端末５に送信する。キオスク端末５における暗号化／復号化部ではホスト認証AデータＤ２を鍵として１６バイトづつ復号化し、復号化したプレーヤＩＤを記憶部に保存する。また、プレーヤ６ａからのプレーヤＩＤの送信がない場合には、再度、プレーヤＩＤの要求をし、それでも送信がない場合には、プレーヤへの処理を中止する。

【００３１】次いでキオスク端末５がプレーヤ６ａに対して所定の送信フォーム「7」の転送履歴送信要求を送信すると、プレーヤ６ａでは、制御部６ａ-10内の記憶部６ａｍに前述の受信した履歴数、履歴転送回数、コンテンツ販売ＩＤ、転送元ＩＤ、転送制御データ等の転送履歴が有るか否かを検出し、有る場合には暗号化／復号化部６ａ-6で販売コンテンツ受信順に全転送履歴をホスト認証AデータＤ２を鍵としてＤＥＳ暗号化し、キオスク端末５に対して所定の送信フォーム「8」で転送履歴を送信し、キオスク端末５では、受信した転送履歴をホスト認証AデータＤ２を鍵としてＤＥＳ復号化する。次いでキオスク端末５がプレーヤ６ａに対して所定の送信フォーム「9」の転送履歴削除要求を送信すると、プレーヤ６ａでは転送履歴を削除する。また、転送履歴削除要求が無い場合には、全転送履歴の履歴転送回数を１カウントアップして保存する。そして、プレーヤ６ａが転送履歴を削除した場合にはキオスク端末５に対して所定の送信フォーム「１０」の転送履歴削除通知を送信する。従って、これらの転送履歴は、後に課金管理サーバ８に供給され、そこで著作権管理のための情報等に使用される。

【００３２】次いでキオスク端末５における操作に応じて「コンテンツ転送」、「編集データ転送」に選択的に移行する。「コンテンツ転送」が選択された場合には、キオスク端末５がプレーヤ６ａに対し、所定の送信フォーム「１１」のチケット残高送信要求がなされる。プレーヤ６ａの制御部６ａ-10では電子財布６ａ-2におけるチケットの残高を照合し、この残高を暗号化／復号化部６ａ-6においてホスト認証に使用した認証AデータＤ２を鍵として１６バイトづつＤＥＳ暗号化して、このデータを送信フォーム「１２」によりキオスク端末５に送信し、キオスク端末５の暗号化／復号化部でホスト認証で受信した認証AデータＤ２を鍵として１６バイトづつＤＥＳ復号化し、チケット残高を記憶部に保存する。このとき、残金のない場合には、処理を中止するか、クレジット方式の場合にはその情報を課金管理サーバ８に送信して周知の手続き処理が行われる。チケット残高の受信が得られない場合には、再度前述の残高送信要求の処理を実行し、送信がない場合にはプレーヤ処理を中止する。

【００３３】前記の処理において、残高送信があった場合には、次いでプレーヤ６ａに送信フォーム「１５」の空き容量送信要求をする。プレーヤ６ａでは記憶部６ａ-5内に記憶されているデータのヘッダー／コンテンツ空き容量を照合して、キオスク端末５に送信フォーム「１６」によりその照合結果を送信する。キオスク端末５ではこの空き容量を記憶部に記憶する。空き容量がない場合には処理を中止するか、キオスク端末側で空き容量を確保するための制御信号を出力することになる。また、送信がない場合には前述の処理を再度実行し、それでも送信がない場合にはプレイ処理を中止する。

【００３４】次いでキオスク端末５からプレーヤ６ａに所定の送信フォーム「１７」の内蔵コンテンツ販売ＩＤの送信要求を行う。プレーヤ６ａにおける記憶部６ａ-5内に内蔵コンテンツ販売ＩＤが記録されている場合には、全コンテンツ販売ＩＤをホスト認証に使用した認証AデータＤ２を鍵として１６バイトづつＤＥＳ暗号化し、このデータを所定の送信フォーム「１８」によりキオスク端末５に送信する。内蔵コンテンツ販売ＩＤが無い場合にはその旨を所定の送信フォーム「１８」により送信する。

【００３５】次いでキオスク端末５がプレーヤ６ａに対して所定の送信フォーム「１９」、「２０」、「２１」でそれぞれ販売ヘッダ、販売サブヘッダ、コンテンツデータを順次を送信すると、プレーヤ６ａがこれらに応答してキオスク端末５に対して所定の送信フォーム「２２」の各データ受信通知を送信する。次いでキオスク端末５では、記憶部に記憶されている販売ヘッダ内の１次暗号化再生鍵データを先に送信されてきたプレーヤ６ａのプレーヤＩＤを鍵として２次暗号化し、この２次暗号化鍵データをプレーヤ６ａに対して所定の送信フォーム「２５」で送信する。プレーヤ６ａでは、この２次暗号化鍵データを記憶部６ａ-5の販売ヘッダの鍵データ保存領域に格納する。そして、電子財布部６ａ-2により販売チケット数分減額し、受信コンテンツの転送履歴を制御部６ａ-10内の記憶部ｍに記録する。そして、これらの

処理が終了すると、所定の送信フォーム「２６」の再生鍵データ受信通知をキオスク端末５に送信し、キオスク端末５とプレーヤ６ａの間のＩＥＥＥ１３９４インタフェースを切断する。

【００３６】また、一方、図１７は、前記の「コンテンツ転送」の代わりに「編集データ転送」が選ばれたときのフローチャートで、同図に示すように、このモードが選択されると、キオスク端末５がプレーヤ６ａに対して所定の送信フォーム「３０」の編集データ送信要求を送信すると、プレーヤ６ａがこれに応答して編集対象の曲を、十進数で１から始まる再生順番、その曲データ長、曲名、アーティスト名の順に、所定の送信フォーム「３１」でキオスク端末５に送信する。次いでキオスク端末５ではこの送信データを記憶部に保存し、プレーヤ６ａに対して所定の送信フォーム「３２」のコンテンツ削除データを送信する。プレーヤ６ａではこのデータに基づいて受信削除再生順番の曲の再生リストからの削除、及び販売コンテンツデータと販売サブヘッダの消去、販売ヘッダの再転送禁止処理又は消去を行う。そして、キオスク端末５に対して所定の送信フォーム「３３」の販売コンテンツデータ削除通知を送信する。次いでキオスク端末５がプレーヤ６ａに対して所定の送信フォーム「１５」の空き容量送信要求を送信すると、プレーヤ６ａがこれに応答してキオスク端末５に対して所定の送信フォーム「１６」の空き容量を送信する。

【００３７】次いでキオスク端末５は、前記の編集対象のデータに基づいて、再生順番の並び替え等の編集を行い、この編集済みデータをプレーヤ６ａに対して所定の送信フォーム「３４」で送信する。プレーヤ６ａでは、これに基づき旧再生順番を新再生順番に変更し、その後、キオスク端末５に対して所定の送信フォーム「３５」の編集済データ受信通知をプレーヤ６ａに送信する。そして、キオスク端末５とプレーヤ６ａの間のＩＥＥＥ１３９４インタフェースを切断する。

【００３８】次に、前述のインターネット方式におけるＷｅｂサーバ９とＰＣクライアント１０の間、及びＰＣクライアント１０とプレーヤ６ａの間の通信手順につき、図１８～図２３を参照して説明する。まず、図１８に示すようにＰＣクライアント１０とプレーヤ６ａがＩＥＥＥ１３９４インタフェースを介して接続されると、ＰＣクライアント１０がプレーヤ６ａに対して所定の送信フォーム「３８」のプレーヤ認証Ｂデータを送信し、プレーヤ６ａがこれに応答してＰＣクライアント１０に対して所定の送信フォーム「３９」の返信プレーヤ認証Ｂデータとホスト認証Ｂデータを送信する。次いでＰＣクライアント１０がプレーヤ６ａに対して所定の送信フォーム「４０」の返信ホスト認証Ｂデータを送信すると、プレーヤ６ａがこれに応答してＰＣクライアント１０に対して所定の送信フォーム「４１」のホスト認証Ｂ結果を送信する。

【００３９】次いでＰＣクライアント１０がプレーヤ６ａに対して所定の送信フォーム「１１」のチケット残高送信要求を送信すると、プレーヤ６ａがこれに応答してＰＣクライアント１０に対して所定の送信フォーム「１２」のチケット残高を送信する。次いでＰＣクライアント１０がプレーヤ６ａに対して所定の送信フォーム「１５」のメモリの空き容量送信要求を送信すると、プレーヤ６ａがこれに応答してＰＣクライアント１０に対して所定の送信フォーム「１６」の空き容量を送信する。次いでＰＣクライアント１０がプレーヤ６ａに対して所定の送信フォーム「１７」の、メモリに既にダウンロードされて記憶されている内蔵コンテンツ販売ＩＤの送信を要求すると、プレーヤ６ａがこれに応答してＰＣクライアント１０に対して所定の送信フォーム「１８」の内蔵コンテンツ販売ＩＤを送信する。次いで所定のフォーム「３４」，「３５」により前記の図１７における販売キオスクとプレーヤ間におけると同様の編集データの要求と送信が行われる。次いでユーザなどがＰＣクライアント１０を介して指示することにより「コンテンツ選択・購入」、「チケット購入」、「コンテンツ編集・削除」の各処理に選択的に移行する。

【００４０】尚、前述のＰＣクライアント１０とプレーヤ６ａとにおける認証方式は、前述の図１１で説明したキオスク端末５とプレーヤ６ａとにおける処理とほぼ同様で、その相違する点は認証データの生成方法で、共通鍵データＫ５を用いて暗号化された返信プレーヤ認証Ｂデータを生成する点と、共通鍵データＫ６を用いて返信ホスト認証Ｂデータを生成する点である。前述の場合では認証Ａデータを用いて互いの機器を認証するようにしたが、特に、この場合のＰＣクライアント１０間との認証データは、データの流出が懸念されることから他とは異なる認証データを用いている。従って、更に他の機器間で認証データの流出が懸念されるようなら、他の機器毎に認証データを異ならせても良い。

【００４１】また、一方、「コンテンツ選択・購入」が選択された場合には、図１９に示すようにクライアント１０とプレーヤ６ａの間で上記の「チケット残高」、「空き容量」及び「内蔵コンテンツ販売ＩＤ」のやり取りを再度行う。次いでクライアント１０がサーバ９に対してコンテンツ購入要求情報を送信し、次いでサーバ９がクライアント１０に対して販売内容チェック結果を送信する。尚、前記の残高送信データや内蔵コンテンツＩＤを送信するときには、ホスト認証Ｂデータを鍵としてＤＥＳ暗号化するようにしている。

【００４２】次いでクライアント１０がＷｅｂサーバ９に対してコンテンツ購入要求を送信すると、Ｗｅｂサーバ９がクライアント１０に対してプレーヤ認証Ａデータを送信し、次いでクライアント１０がプレーヤ６ａに対してこのプレーヤ認証Ａデータを送信する。次いでプレーヤ６ａがこれに応答してクライアント１０に対して返

信プレーヤ認証Aデータとホスト認証データを送信し、次いでクライアント１０がＷｅｂサーバ９に対してこの返信プレーヤ認証Aデータとホスト認証Aデータを送信する。

【００４３】次いでサーバ９がクライアント１０に対して返信ホスト認証A送信データを送信し、次いでクライアント１０がプレーヤ６ａに対してこの返信ホスト認証A送信データを送信する。次いでプレーヤ６ａがこれに応答してクライアント１０に対して返信ホスト認証Aデータの結果を送信し、次いでクライアント１０がサーバ９に対してこの結果を送信する。

【００４４】次に、図２０に示すように、Ｗｅｂサーバ９がＰＣクライアント１０に対して所定の送信フォーム「5」、「１１」、「１５」、「１７」、「7」でそれぞれプレーヤＩＤ送信要求、チケット残高送信要求、空き容量送信要求、内蔵コンテンツ販売ＩＤ送信要求、転送履歴送信要求を送信する。次いでＰＣクライアント１０がプレーヤ６ａに対して所定の送信フォーム「5」のプレーヤＩＤ送信要求を送信するとプレーヤ６ａがこれに応答してＰＣクライアント１０に対して所定の送信フォーム「6」のプレーヤＩＤを送信し、ＰＣクライアント１０がプレーヤ６ａに対して所定の送信フォーム「１１」のチケット残高送信要求を送信するとプレーヤ６ａがこれに応答してＰＣクライアント１０に対して所定の送信フォーム「１２」のチケット残高を送信する。

【００４５】また、ＰＣクライアント１０がプレーヤ６ａに対して所定の送信フォーム「１５」の空き容量送信要求を送信するとプレーヤ６ａがこれに応答してＰＣクライアント１０に対して所定の送信フォーム「１６」の空き容量を送信し、ＰＣクライアント１０がプレーヤ６ａに対して所定の送信フォーム「１７」の内蔵コンテンツ販売ＩＤ送信要求を送信するとプレーヤ６ａがこれに応答してＰＣクライアント１０に対して所定の送信フォーム「１８」の内蔵コンテンツ販売ＩＤを送信し、ＰＣクライアント１０がプレーヤ６ａに対して所定の送信フォーム「7」の転送履歴送信要求を送信するとプレーヤ６ａがこれに応答してＰＣクライアント１０に対して所定の送信フォーム「8」の転送履歴を送信する。ＰＣクライアント１０はＷｅｂサーバ９に対して、これらの所定の送信フォーム「6」、「１２」、「１６」、「１８」、「8」でそれぞれプレーヤＩＤ、チケット残高、空き容量、内蔵コンテンツ販売ＩＤ、転送履歴を送信する。そして、この転送履歴は前述したように課金管理サーバ８に送信されることになる。

【００４６】次いでＷｅｂサーバ９が転送履歴を回収すると、ＰＣクライアント１０に対して所定の送信フォーム「9」の転送履歴削除要求を送信するとＰＣクライアント１０がプレーヤ６ａに対してこの送信フォーム「9」の転送履歴削除要求を送信し、プレーヤ６ａがこれに応答して制御部６ａ-10内の記憶部ｍに記憶されている転送履歴を削除する。そして、ＰＣクライアント１０に対して所定の送信フォーム「１０」の転送履歴削除通知を送信するとＰＣクライアント１０がＷｅｂサーバ９に対してこの送信フォーム「１０」の転送履歴削除通知を送信する。これらのデータの送信は、プレーヤ６ａにおいて、空き容量の送信を除き、ホスト認証Aデータを鍵としてＤＥＳ暗号化されて送信される。

【００４７】次いでＷｅｂサーバ９がＰＣクライアント１０に対して送信フォーム「１９」、「２０」、「２１」でそれぞれ販売ヘッダ、販売サブヘッダ、販売コンテンツデータを送信する。次いでＰＣクライアント１０がプレーヤ６ａに対して送信フォーム「１９」、「２０」、「２１」でそれぞれ販売ヘッダ、販売サブヘッダ、販売コンテンツデータを送信するとプレーヤ６ａは、これらのデータを記憶部６ａ-5に記憶する。そして、ＰＣクライアント１０に対して送信フォーム「２２」の各データ受信通知を送信し、ＰＣクライアント１０がに対してこの送信フォーム「２２」のデータ受信通知を送信する。

【００４８】次いで図２１に示すようにＷｅｂサーバ９がＰＣクライアント１０に対して送信フォーム「２５」の再生鍵データを送信すると、ＰＣクライアント１０がプレーヤ６ａに対してこの送信フォーム「２５」の再生鍵データを送信する。次いでプレーヤ６ａは、受信再生鍵データを販売ヘッダの鍵データ保存領域に格納すると共に、購入チケット数分の減額、受信コンテンツデータの転送履歴等の記録を行いＰＣクライアント１０に対して送信フォーム「２６」の再生鍵データ受信通知を送信し、ＰＣクライアント１０がＷｅｂサーバ９に対してこの送信フォーム「２６」の再生鍵データ受信通知を送信する。そして、ＰＣクライアント１０とプレーヤ６ａの間のＩＥＥＥ１３９４インタフェースを切断する。

【００４９】次に、図１８において「コンテンツ編集・削除」が選択された場合につき、図２２を参照して説明する。この処理では、サーバ９とクライアント１０の間の回線は接続されず、クライアント１０とプレーヤ６ａの間のみが接続された状態で行われる。まず、クライアント（ホスト側）１０がプレーヤ６ａに対してコンテンツ削除データを送信すると、プレーヤ６ａがこれに基づいて図１７のプレーヤ処理１１と同様にしてデータの削除をする。そして、クライアント１０に対してコンテンツ削除通知を送信する。

【００５０】次に、ここで、クライアント１０において、編集処理が行われる。その処理を図２３を参照して説明する。まず、プレーヤ６ａから転送された編集対象のコンテンツを表示し（ステップＳ１）、次いで編集項目が入力されると（ステップＳ２）、入力項目に応じて編集対象のコンテンツを編集する（ステップＳ３）。そして、図２２に示すように、前記の編集済データが送信されると、プレーヤ６ａがこれに応答してクライアント

１０に対して編集済データ受信通知を送信する。

【００５１】次に、図２４～図２６を参照して図１９～図２１に対応した別の「コンテンツ選択・購入」の実施例につき説明する。すなわち、図１８において、「コンテンツ選択・購入」が選択された場合には、図２４に示すようにクライアント１０がサーバ９に対してコンテンツ購入要求情報を送信し、次いでサーバ９がクライアント１０に対して販売内容チェック結果を送信する。次いでクライアント１０がサーバ９に対してコンテンツ購入要求を送信すると、サーバ９がプレーヤ認証Ａデータをクライアント１０をスルーしてプレーヤ６ａに送信し、プレーヤ６ａがこれに応答して返信プレーヤ認証Ａデータとホスト認証データをクライアント１０をスルーしてサーバ９に送信する。次いでサーバ９が返信ホスト認証Ａ送信データをクライアント１０をスルーしてプレーヤ６ａに送信すると、プレーヤ６ａがこれに応答して返信ホスト認証Ａ送信データの結果をクライアント１０をスルーしてサーバ９に送信する。

【００５２】次に、図２５に示すように、サーバ９がプレーヤＩＤ送信要求、チケット残高送信要求、空き容量送信要求、内蔵コンテンツ販売ＩＤ送信要求、転送履歴送信要求をクライアント１０をスルーしてプレーヤ６ａに送信すると、プレーヤ６ａがこれに応答してプレーヤＩＤ、チケット残高、空き容量、内蔵コンテンツ販売ＩＤ、転送履歴をクライアント１０をスルーしてサーバ９に送信する。

【００５３】次いでサーバ９が転送履歴削除要求をクライアント１０をスルーしてプレーヤ６ａに対して送信すると、プレーヤ６ａがこれに応答して転送履歴削除通知をクライアント１０をスルーしてサーバ９に送信する。次いでサーバ９が販売ヘッダ、販売サブヘッダ、販売コンテンツデータをクライアント１０をスルーしてプレーヤ６ａに送信すると、プレーヤ６ａがこれに応答して各データ受信通知をクライアント１０をスルーしてサーバ９に送信する。次いで図２６に示すようにサーバ９が再生鍵データをクライアント１０をスルーしてプレーヤ６ａに対して送信すると、プレーヤ６ａがこれに応答して再生鍵データ受信通知をクライアント１０をスルーしてサーバ９に送信する。そして、クライアント１０とプレーヤ６ａの間のＩＥＥＥ１３９４インタフェースを切断する。

【００５４】次に、図２７を参照してプレーヤ６ａ、６ｂ間におけるデータ転送の処理につき説明する。まず、プレーヤ（ホスト側）６ａの暗号化部６ａ-5において例えば８バイトの乱数認証ＡデータＤ１を作成し、共通鍵データＫ１によりＤＥＳ暗号化し、この暗号化された認証ＡデータＤ１を８バイトの所定の送信フォーム「１」でデータ転送インターフェース６ａ-1を介してプレーヤ６ｂに送信する。プレーヤ６ｂでは、このプレーヤ認証ＡデータＤ１をデータ転送インターフェース６ｂ-1を介して受信し、暗号化／復号化部６ｂ-6において、共通鍵データＫ１によりＤＥＳ復号化し、この復号化で得られた認証ＡデータＤ１を他の共通鍵データＫ２によりＤＥＳ暗号化し、返信プレーヤ認証Ａデータを作成する。それと同時に、８バイトの乱数認証ＡデータＤ３を作成し、この認証ＡデータＤ３を更に他の共通鍵データＫ３によりＤＥＳ暗号化し、このデータをホスト認証Ａデータとし、所定送信フォーム「２」でホスト認証Ａデータと前記返信プレーヤ認証Ａデータとを再びプレーヤ６ａに返信する。

【００５５】プレーヤ６ａでは、データ転送インターフェース６ａ-1を介して返信プレーヤ認証Ａデータとホスト認証Ａデータとを受信し、これらを暗号化／復号化部６ａ-6に供給し、ここで、返信プレーヤ認証Ａデータが共通鍵データＫ３によりＤＥＳ復号化され、この復号化された認証ＡデータＤ１と送信認証ＡデータＤ１とが制御部６ａ-10において照合される。照合の結果、不一致の場合には、このプレーヤ６ａ側において行った前述の処理を２回まで再度実行する。それでも不一致する場合にはプレーヤ６ａにおける処理を中止する。

【００５６】また、一方、一致した場合には、受信ホスト認証Ａデータを共通鍵データＫ３によりＤＥＳ復号化し、この復号化で得られた認証データＤ２を、他の共通鍵データＫ４によりＤＥＳ暗号化し、返信ホスト認証Ａデータとし、このデータを所定の送信フォーム「３」によりプレーヤ６ｂに送信する。プレーヤ６ｂの暗号化／復号化部６ｂ-6では、この返信ホスト認証Ａデータを共通鍵データ４によりＤＥＳ復号化し、復号化された認証ＡデータＤ２を得て、この復号化された認証ＡデータＤ２と送信ホスト認証Ａデータとを制御部６ｂ-10において照合し、一致の場合には所定の送信フォーム「４」のホスト認証をプレーヤ６ａに送信し、その後の処理を受け付ける。また、一方、認証不一致の場合には、所定の送信フォーム「４」の認証不可をプレーヤ６ａに送信し、これ以降の処理の受付を禁止する。

【００５７】次いでプレーヤ６ａからプレーヤ６ｂに対し、所定の送信フォーム「５」のプレーヤＩＤの送信要求がなされる。これを受信したプレーヤ６ｂ側では暗号化／復号化部６ｂ-7において、自己プレーヤＩＤをホスト認証に使用した認証ＡデータＤ２を鍵として１６バイトづつＤＥＳ暗号化し、所定の送信フォーム「６」でデータをプレーヤ６ａに送信する。プレーヤ６ａにおける暗号化／復号化部６ａ-6ではホスト認証ＡデータＤ２を鍵として１６バイトづつ復号化し、復号化したプレーヤＩＤを記憶部ｍに保存する。また、プレーヤ６ｂからのプレーヤＩＤの送信がない場合には、再度、プレーヤＩＤの要求をし、それでも送信がない場合には、プレーヤ処理を中止する。

【００５８】次いでプレーヤ６ａからプレーヤ６ｂに対し、所定の送信フォーム「１１」のチケット残高送信要

求がなされる。プレーヤ６ｂの制御部６ｂ-10では電子財布６ｂ-2におけるチケットの残高を照合し、この残高を暗号化／復号化部６ｂ-6においてホスト認証に使用した認証ＡデータＤ２を鍵として１６バイトづつＤＥＳ暗号化して、このデータを送信フォーム「１２」によりプレーヤ６ａに送信し、プレーヤ６ａの暗号化／復号化部６ａ-6でホスト認証で受信した認証ＡデータＤ２を鍵として１６バイトづつＤＥＳ復号化し、チケット残高を記憶部ｍに保存する。このとき、チケット残高の受信が得られない場合には、再度前述の残高送信要求の処理を実行し、送信がない場合にはプレーヤ処理を中止する。

【００５９】残高送信があれば、次に、プレーヤ６ｂに所定の送信フォーム「１５」の空き容量送信要求をする。プレーヤ６ｂでは記憶部６ｂ-5内に記憶されているデータのヘッダー／コンテンツ空き容量を照合して、プレーヤ６ａに所定の送信フォーム「１６」によりその照合結果を送信する。プレーヤ６ａではこの空き容量を記憶部ｍに記憶する。送信がない場合には前述の処理を再度実行し、それでも送信がない場合にはプレイ処理を中止する。

【００６０】次いでプレーヤ６ａからプレーヤ６ｂに所定の送信フォーム「１７」の内蔵コンテンツ販売ＩＤの送信要求を行う。プレーヤ６ｂにおける記憶部６ｂ-5内にすでに転送済みの内蔵コンテンツ販売ＩＤが記録されているには、全コンテンツ販売ＩＤをホスト認証に使用した認証ＡデータＤ２を鍵として１６バイトづつＤＥＳ暗号化し、このデータを所定の送信フォーム「１８」によりプレーヤ６ａに送信する。内蔵コンテンツ販売ＩＤが無い場合には、その旨を所定の送信フォーム「１８」により送信する。

【００６１】プレーヤ６ａでは、制御部６ａ-6において、記憶部６ａ-5に記憶されている転送コンテンツ販売ＩＤとプレーヤ６ｂから送信されてきた内蔵コンテンツ販売ＩＤとを照合する。同一コンテンツ販売ＩＤがある場合にはプレーヤ６ａの処理を中止する。また、同一コンテンツ販売ＩＤが無い場合には、転送コンテンツ販売ヘッダ内の転送制御データ再転送世代数を確認する。確認の結果、転送世代数が［００００：コピー不可］である場合には、その旨を再生部６ａ-8を通じて表示部６ａ-3において、［コピー不可］を表示して処理を中止すると共に、プレーヤ６ｂ側も所定時間内にデータの受信が得られないと同様に表示部６ｂ-3に［コピー不可］を表示する。

【００６２】また、転送世代数が［０００１］以上である場合には、転送制御データの再転送世代数を１カウントダウンし、転送コンテンツの再生鍵データを除く販売ヘッダをプレーヤ６ｂの認証時に使用した認証ＡデータＤ１を鍵としてＤＥＳ暗号化して、所定の送信フォーム［１９］でプレーヤ６ｂに送信する。プレーヤ６ｂでは、これを受信し販売ヘッダを認証ＡデータＤ１を用いてＤＥＳ復号化し、記憶部６ｂ-5に記憶すると共に、受信通知をプレーヤ６ｂに送信する。

【００６３】また、プレーヤ６ａでは、記憶部６ａ-5に販売サブヘッダがある場合には前記の販売ヘッダの場合と同様にプレーヤ６ｂの認証時に使用した認証ＡデータＤ１を鍵としてＤＥＳ暗号化して、プレーヤ６ａに対して所定の送信フォーム［２０］で送信する。プレーヤ６ａでは、この販売サブヘッダを認証ＡデータＤ１を鍵としてＤＥＳ復号化し、記憶部６ｂ-5に記憶する。また、プレーヤ６ａに販売サブヘッダ情報が無い場合には、次の所定の送信フォーム［２１］で前述の方式で暗号化されたコンテンツデータを送信する。プレーヤ６ｂでは、このコンテンツデータを記憶部６ｂ-5に記憶し、所定の送信フォーム［２２］で受信通知を返送する。

【００６４】次いでプレーヤ６ａでは、記憶部６ｂ-5における転送販売ヘッダ再生鍵保存領域の２次暗号化再生鍵データを、暗号化／復号化部６ａ-6において自己プレーヤ（６ａ）のＩＤを鍵としてＤＥＳ復号化し、１次暗号化再生鍵データを復号する。そして、この１次暗号化再生鍵データを、転送先であるプレーヤ６ｂのＩＤを鍵として再び２次ＤＥＳ暗号化処理を行い、この２次暗号化された再生鍵データを所定の送信フォーム［２５］でプレーヤ６ｂに送信する。プレーヤ６ｂでは、この２次暗号化鍵データを記憶部６ｂ-5の販売ヘッダの鍵データ保存領域に格納する。そして、電子財布部６ｂ-2により販売チケット数分減額し、受信コンテンツの前述の転送履歴を制御部内６ｂ-1の記憶部ｍに記録する。そして、これらの処理が終了すると、所定の送信フォーム「２６」の再生鍵データ受信通知をプレーヤ６ａに送信し、プレーヤ６ａとプレーヤ６ｂの間のＩＥＥＥ１３９４インタフェースを切断する。

【００６５】次に、図２８，図２９は、前述のプレーヤ６ａ及びプレーヤ６ｂ間におけるデータ転送の別の実施例で、前述の実施例と異なる点は、特に、プレーヤ６ｂから転送履歴をもらう点である。所定の送信フォーム［１］～［６］までは、前述の実施例である図２７の説明と同一であるため説明を省略し、送信フォーム［７］より説明する。この送信フォーム［７］により、プレーヤ６ａからプレーヤ６ｂに対して転送履歴の要求を行う。プレーヤ６ｂでは、制御部６ｂ-10内の記憶部ｍに転送履歴が有るか否かを検出し、有る場合には暗号化／復号化部６ｂ-6で販売コンテンツ受信順に全転送履歴をホスト認証ＡデータＤ２を鍵としてＤＥＳ暗号化し、応答してプレーヤ６ａに対して所定の送信フォーム「８」で転送履歴を送信し、プレーヤ６ａでは、暗号化／復号化部６ａ-6において転送履歴をホスト認証ＡデータＤ２を鍵としてＤＥＳ復号化する。そして、制御部６ａ-10では、これらのデータに基づきコピーが可能な否かをチェックし、その旨を所定のフォーム［９］でプレーヤ６ｂに送信する。プレーヤ６ｂでは、特に、コピーができ

ない場合には、再生部６ｂ-8を通じて表示部６ｂ-3によりその旨を表示する。また、コピー可の場合には全転送履歴の履歴転送回数を１カウントアップして保存する。そして、所定の送信フォーム「１０」により前記のデータの受信をプレーヤ６ａに送信する。

【００６６】そして、コピー可と判断された場合には、「コンテンツ転送」処理へと進行し、プレーヤ６ａからプレーヤ６ｂに対し、所定の送信フォーム「１１」のチケット残高送信要求がなされる。プレーヤ６ｂの制御部６ａ-10では電子財布６ｂ-2におけるチケットの残高を照合し、この残高を暗号化／復号化部６ｂ-6においてホスト認証に使用した認証ＡデータＤ２を鍵として１６バイトづつＤＥＳ暗号化して、このデータを送信フォーム「１２」によりプレーヤ６ａに送信し、プレーヤ６ａの暗号化／復号化部６ａ-6でホスト認証で受信した認証ＡデータＤ２を鍵として１６バイトづつＤＥＳ復号化し、チケット残高を記憶部６ａ-5に保存する。このとき、チケット残高の受信が得られない場合には、再度前述の残高送信要求の処理を実行し、送信がない場合にはプレーヤ処理を中止する。

【００６７】前記の処理において、残高送信があった場合には、次に、プレーヤ６ｂに送信フォーム「１５」の空き容量送信要求をする。プレーヤ６ｂでは記憶部m内に記憶されているデータのヘッダー／コンテンツ空き容量を照合して、プレーヤ６ａに送信フォーム「１６」によりその照合結果を送信する。プレーヤ６ａではこの空き容量を記憶部に記憶する。送信がない場合には前述の処理を再度実行し、それでも送信がない場合にはプレイ処理を中止する。

【００６８】次に、プレーヤ６ａからプレーヤ６ｂに所定の送信フォーム「１７」の内蔵コンテンツ販売ＩＤの送信要求を行う。プレーヤ６ｂにおける記憶部６ｂ-5内に内蔵コンテンツ販売ＩＤが記録されている場合には、全コンテンツ販売ＩＤをホスト認証に使用した認証ＡデータＤ２を鍵として１６バイトづつＤＥＳ暗号化し、このデータを所定の送信フォーム「１８」によりプレーヤ６ａに送信する。内蔵コンテンツ販売ＩＤが無い場合にはその旨を所定の送信フォーム「１８」により送信する。

【００６９】次いで、プレーヤ６ａがプレーヤ６ｂに対して所定の送信フォーム「１９」、「２０」、「２１」でそれぞれ販売ヘッダ、販売サブヘッダ、コンテンツデータを順次を送信すると、プレーヤ６ｂがこれらに応答してプレーヤ６ａに対して所定の送信フォーム「２２」の各データ受信通知を送信する。次いで、プレーヤ６ａでは、記憶部６ｂ-5における転送販売ヘッダ再生鍵保存領域の２次暗号化再生鍵データを、暗号化／復号化部６ａ-6において自己プレーヤ（６ａ）のＩＤを鍵としてＤＥＳ復号化し、１次暗号化再生鍵データを復号する。そして、この１次暗号化再生鍵データを、転送先であるプレーヤ６ｂのＩＤを鍵として再び２次ＤＥＳ暗号化処理を行い、この２次暗号化された再生鍵データを所定の送信フォーム［２５］でプレーヤ６ｂに送信する。プレーヤ６ｂでは、この２次暗号化鍵データを記憶部６ｂ-5の販売ヘッダの鍵データ保存領域に格納する。そして、電子財布部６ｂ-2により販売チケット数分減額し、受信コンテンツの転送履歴を記憶部６ｍに記録する。そして、これらの処理が終了すると、所定の送信フォーム「２６」の再生鍵データ受信通知をキオスク端末５に送信し、キオスク端末５とプレーヤ６ａの間のＩＥＥＥ１３９４インタフェースを切断する。

【００７０】尚、前述の説明において、決裁ボックス７とプレーヤ６ａ，６ｂ間のデータ転送手順を詳述しなかったが、図１１で示したキオスク・プレーヤ間データ転送手順における［コンテンツ転送］及び［編集データ転送］の選択のステップを除き所定の送信フォーム［１］～［１２］までの処理がほぼ同じで、その後に処理として例えば前述の電子チケットが発行されるようになっている。従って、互いの機器の認証方式やプレーヤＩＤを送信する際の暗号化方式も同様である。

【００７１】また、前述の鍵データは、プレーヤＩＤで暗号化し、復号化するようにしているが、例えば、プレーヤ６ａ，ｂ内のコンテンツデータを記録する記憶部６ａ-5，６ｂ-5が着脱自在のメモリディバイスのような記録媒体であるような場合には、記録媒体にＩＤを付与して、このＩＤに基づいて暗号化・復号化するようにしても良い。また、このように記憶部６ｂ-5が着脱自在なような場合には、コンテンツデータを前記のように再生鍵でＸＯＲ演算で暗号化したまま状態で所定領域に記録すると共に、ヘッダ情報を暗号化したままの所定領域に記録するようにしても良い。

【００７２】更に、前述の編集処理は、販売元端末であるキオスク端末及びＰＣクライアントにおいてしか行えないようにしているが、それらに限らずコンテンツデータの改竄が行われないように暗号化されたままのデータを編集する等、著作権管理が工夫された編集装置なら良い。

【００７３】また、更に、図３０はテキストデータのフォーマットを示した図で、テキストデータは図３０（ａ）に示すように複数のテキスト「１」～「Ｎ」により構成され、テキスト「１」～「Ｎ」の各々は、図３０（ｂ）に示すように複数のテキストフレーム「１」～「Ｎ」により構成されている。テキストフレーム「１」～「Ｎ」の各々はともに、オーサリング時にコンテンツデータを暗号化したときと同じ暗号化方式で、再生鍵データと同じ１６バイトで構成されて、３バイトのタイムスタンプと、１バイトのフレーム数と１２バイトのテキストデータにより構成されている。そして、上記の暗号化、復号は、再生鍵データとテキストフレーム「１」～「Ｎ」ずつ、すなわち１６バイトずつに排他的論理和

（ＸＯＲ）演算することにより行われている。

【００７４】

【発明の効果】以上説明したように本発明によれば、コピーが行われないような暗号化を行うと共に、より速い再生速度での再生が要求される例えば実データであるコンテンツデータと、それほど速い処理速度での再生が要求されない例えばヘッダ情報等との暗号化方式を異ならせ、コンテンツデータの方は時間を要せずに復号化できる暗号化方式とし、ヘッダ情報の方は復号化に多少時間を要しても暗号がもれないような複雑な暗号化方式とすることで、再生鍵データが含まれる情報部を今まで以上に知られにくくすると共に、再生タイミングに支障をきたすようなことがないようにする。

【図面の簡単な説明】

【図１】本発明が採用されるキオスク端末を経由するコンテンツ販売システムの一例を示す構成図である。

【図２】本発明が採用されるインターネット形式によるコンテンツ販売システムの例を示す構成図である。

【図３】図１のプレーヤに配信される販売ヘッダの構成を示す説明図である。

【図４】図１のオーサリングにより付与される販売ヘッダの構成を示す説明図である。

【図５】図１のプレーヤに配信される販売サブヘッダの構成を示す説明図である。

【図６】図４及び図５内の転送制御データの構成を示す説明図である。

【図７】図１、図７のオーサリングシステムの１次暗号化処理を示すフローチャートである。

【図８】図１、図７のキオスク端末及びＷｅｂサーバの２次暗号化処理を示すフローチャートである。

【図９】図１、図７のコピー元プレーヤのコピー管理処理と２次暗号化処理を示すフローチャートである。

【図１０】プレーヤの構成概略構成図である。

【図１１】キオスク・プレーヤ間のデータ転送の手順を示す説明図である。

【図１２】図１１の連続した手順を示す説明図である。

【図１３】転送フォームの構成図である。

【図１４】発信元のコードの例を示す図である。

【図１５】コマンドを示す図である。

【図１６】図１５以外のコマンドを示す図である。

【図１７】図１１において、編集データの転送が選択されたときの処理を示す説明図である。

【図１８】インターネットサーバ・インタネットクライアント・プレーヤ間のデータ転送手順を示す説明図である。

【図１９】図１８に連続する説明図である。

【図２０】図１９に連続する説明図である。

【図２１】図２０に連続する説明図である。

【図２２】図１８においてコンテンツ編集・削除が選択されたときの手順を示す説明図である。

【図２３】クライアントの編集処理を説明するための図である。

【図２４】別のコンテンツ選択・購入の他の例で、図１９～図２１に対応する図である。

【図２５】図２４に連続する図である。

【図２６】図２５に連続する図である。

【図２７】プレーヤ・プレーヤ間の転送手順を示す説明図である。

【図２８】プレーヤ・プレーヤ間の他の例の転送手順を示す説明図である。

【図２９】図２８に連続する図である。

【図３０】テキストデータのフォーマットを示す説明図である。

【符号の説明】

１　オーサリングシステム（ホスト）

２　送信サーバ

３　アップリンクセンタ

４　衛星

５　キオスク端末（転送元端末、販売元端末）

６ａ，６ｂ　プレーヤ（転送先端末、販売先端末）

６ａ-1，６ｂ-1　データインター転送フェース

６ａ-2，６ｂ-2　電子財布

６ａ-3，６ｂ-3　表示部

６ａ-4，６ｂ-4　操作部

６ａ-5，６ｂ-5，ｍ　記憶部

６ａ-6，６ｂ-6　暗号化／復号化部

６ａ-7，６ｂ-7　データ圧縮／伸長部

６ａ-8，６ｂ-8　再生部

６ａ-9，６ｂ-9　出力端子

６ａ-10，６ｂ-10　制御部

９　Ｗｅｂサーバ（インターネットサーバ）（転送元端末）

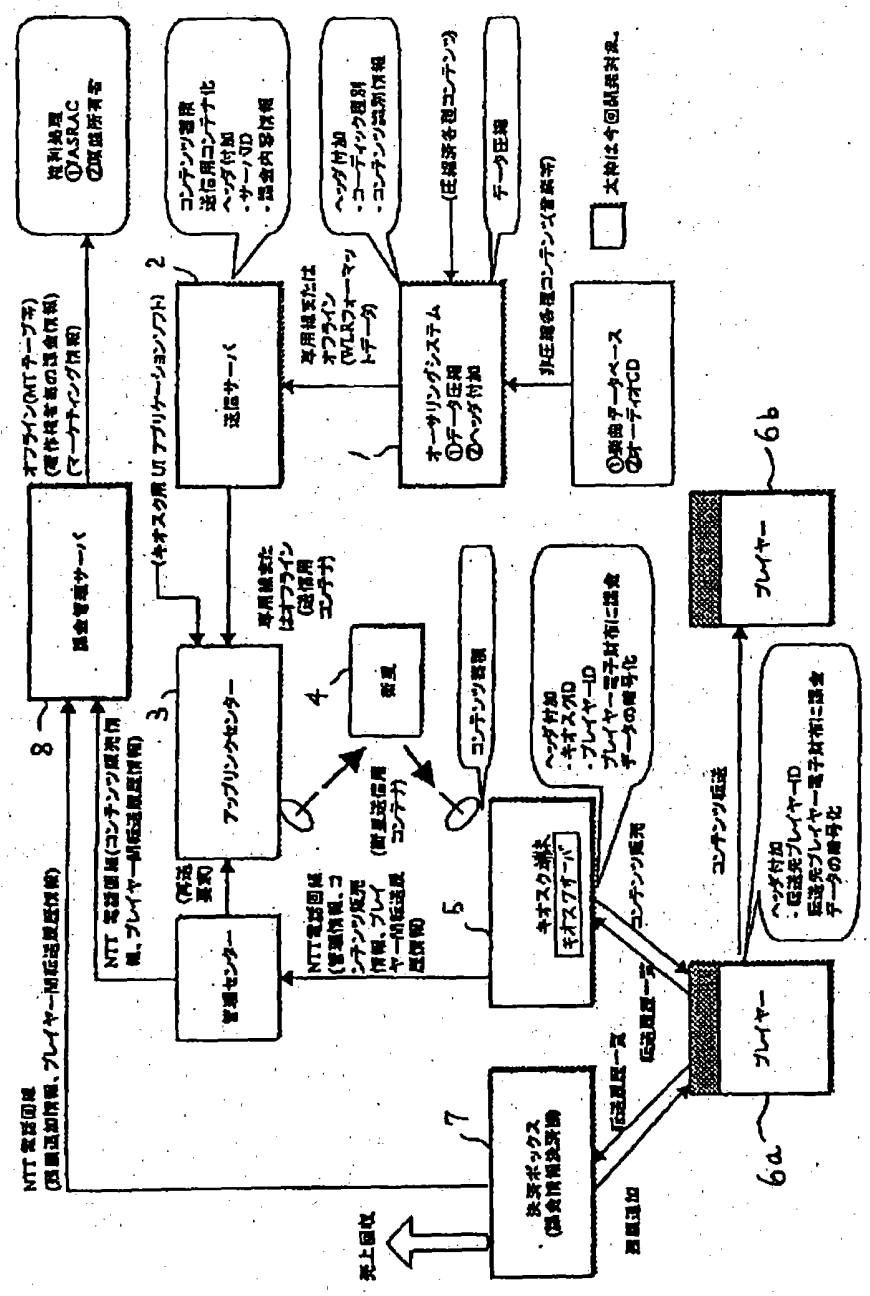
１０　インターネットサービス用ＰＣクライアント

【図１３】

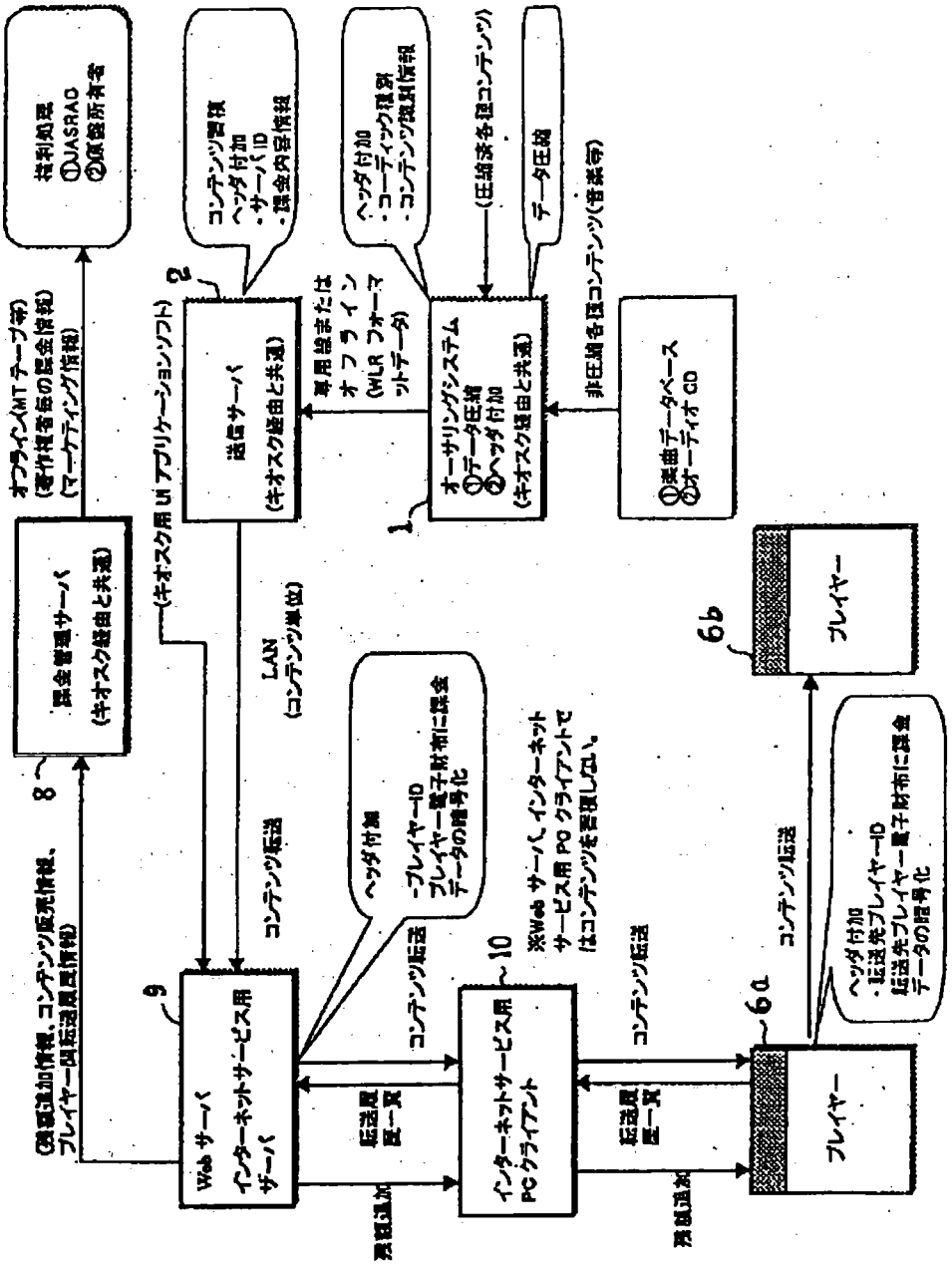
転送フォームの一般形

発信元 1 Byte	ｺﾏﾝﾄﾞ 1 Byte	ﾃﾞｰﾀ長(Byte) 4 Bytes	データ

【図１】


著作権者
①ASRAC
②実演家等
コンテンツ登録
送信用コンテナ化
ヘッダ付加
・サーバID
・課金内容情報
ヘッダ付加
・コーディック識別
・コンテンツ識別情報
(圧縮済み複コンテンツ)
データ圧縮
大枠は今回試験対象。
オフライン(MTテープ等)
(著作権者等の課金情報)
(マーケティング情報)
2
送信サーバ
専用線又は
オフライン
(WLRフォーマット
データ)
オーサリングシステム
①データ圧縮
②ヘッダ付加
非圧縮複複コンテンツ(音楽等)
①楽曲データベース
②オーディオCD
課金管理サーバ
8
(キオスク用 UI アプリケーションソフト)
専用線又は
オフライン
(送信用
コンテナ)
3
アップリンクセンター
4
前置
コンテンツ登録
ヘッダ付加
・キオスクID
・プレイヤーID
プレイヤー電子財布に課金
データの暗号化
プレイヤー
6b
NTT 電話回線(コンテンツ販売情報、プレイヤー別伝送履歴情報)
(再生要求)
管理センター
NTT電話回線
(管理情報、コンテンツ販売情報、プレイヤー別伝送履歴情報)
(前置送信用コンテナ)
5
キオスク端末
キオスクサーバ
コンテンツ販売
コンテンツ伝送
ヘッダ付加
・伝送先プレイヤーID
伝送先プレイヤー電子財布に課金
データの暗号化
プレイヤー
6a
NTT 電話回線
(課金追加情報、プレイヤー別伝送履歴情報)
7
決済ボックス
(課金情報決済機)
売上回収
伝送履歴一覧
伝送履歴一覧
課金追加

【図２】


権利処理
①JASRAC
②原盤所有者
オフライン(MTテープ等)
(著作権者毎の課金情報)
(マーケティング情報)
課金管理サーバ
(キオスク端末と共通)
8
(キオスク用 UI アプリケーションソフト)
送信サーバ
(キオスク端末と共通)
2
コンテンツ管理
ヘッダ付加
・サーバID
・課金内容情報
専用線または
オフライン
(WLR フォーマットデータ)
オーサリングシステム
①データ圧縮
②ヘッダ付加
(キオスク端末と共通)
1
ヘッダ付加
・コーディング種別
・コンテンツ識別情報
(圧縮済各種コンテンツ)
データ圧縮
非圧縮各種コンテンツ(音楽等)
①楽曲データベース
②オーディオ CD
LAN
(コンテンツ単位)
コンテンツ転送
ヘッダ付加
・プレイヤーID
プレイヤー電子財布に課金
データの暗号化
コンテンツ転送
※Web サーバ、インターネット
サービス用 PC クライアントで
はコンテンツを管理しない。
コンテンツ転送
コンテンツ転送
(課金追加情報、コンテンツ販売情報、
プレイヤー(ID)転送履歴情報)
9
Web サーバ
インターネットサービス用
サーバ
10
インターネットサービス用
PC クライアント
転送履歴一覧
転送履歴一覧
課金追加
課金追加
6a
6b
プレイヤー
プレイヤー
ヘッダ付加
・転送先プレイヤーID
転送先プレイヤー電子財布に課金
データの暗号化

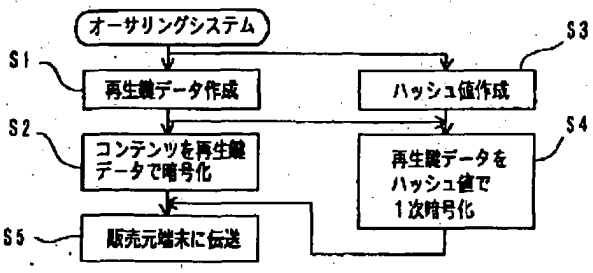
【図３】

販売ヘッダの構成

	b7 b0	b7 b0	b7 b0	b7 b0
0	販売ﾍｯﾀﾞ ﾊﾞｰｼﾞｮﾝ	販売ﾍｯﾀﾞ ｻｲｽﾞ	Reserved (00h)	転送制御データ
4	コンテンツ販売ＩＤ			
8				
12	転送元ＩＤ			
16				
20	販売チケット数		販売ｸﾞﾍｯﾀﾞ数	コンテンツ曲数
24	JAN(POS)コード (52 bits)＋ "0" 12bits			
28				
32 ～ 60	制作タイトル名 (32 Bytes)			
64 ～ 76	制作会社名 (16 Bytes)			
80	１曲目データ長 (4 Bytes)			
84	２曲目データ長 (4 Bytes)			
	N曲目データ長 (4 Bytes)			
	１曲目の曲名			
	２曲目の曲名			
	N曲目の曲名			
	１曲目のアーティスト名			
32N+108 ～ 32N+132	２曲目のアーティスト名			
	N曲目のアーティスト名			
	１曲目の演奏時間 (時、分、秒、フレーム各１Byte)			
	２曲目の演奏時間 (時、分、秒、フレーム各１Byte)			
	N曲目の演奏時間 (時、分、秒、フレーム各１Byte)			
64N+M-K	再生鍵データ保存領域 (K Bytes)			

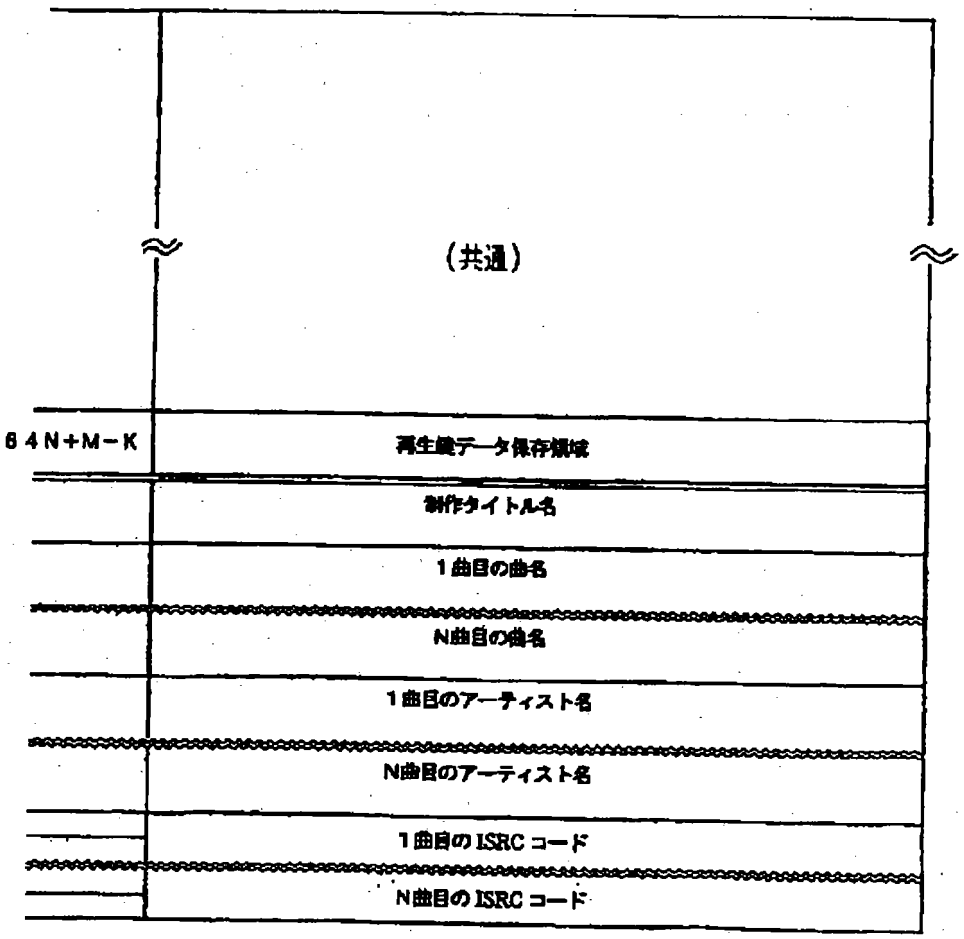
＊ 販売ヘッダ各項目の領域は全てマンダトリーとして割り当てられる。(領域を削除することは不可)
データの無い領域は全て "0" で埋められる。

【図７】



【図４】

マスタリング時の販売ヘッダ



【図６】

b0 ～ b3	再転送世代数	0000: 再転送禁止 0001～1111: 再転送世代数(許可)
b4 ～ b7	再転送禁止	0000: 再転送許可 0001: 再転送禁止 0010～1111: Reserved

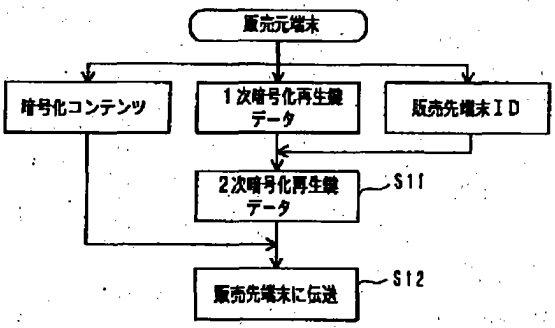
再転送世代数の制御法：初期値に再転送許可世代数を設定。再転送時に１カウントダウンして上書き。
0000 にて再転送禁止

【図５】

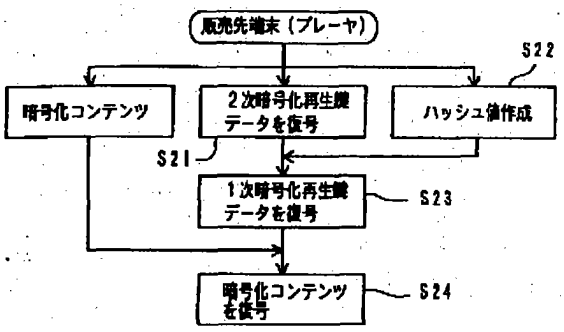
販売サブヘッダ（アルバム内の単曲販売用ヘッダ）の構成

	b7 b0	b7 b0	b7 b0	b7 b0
0	ｻﾌﾞﾍｯﾀﾞ ﾊﾞｰｼﾞｮﾝ	ｻﾌﾞﾍｯﾀﾞ ｻｲｽﾞ	Reserved (00h)	転送制御データ
4	コンテンツ販売ＩＤ			
8				
12	転送元ＩＤ			
16				
20	販売チケット数		00h	指定曲番 (1 Byte)
24	JAN(POS)コード (52 bits)＋ "0" 12bits			
28				
32 ～ 60	制作タイトル名 (32 Bytes)			

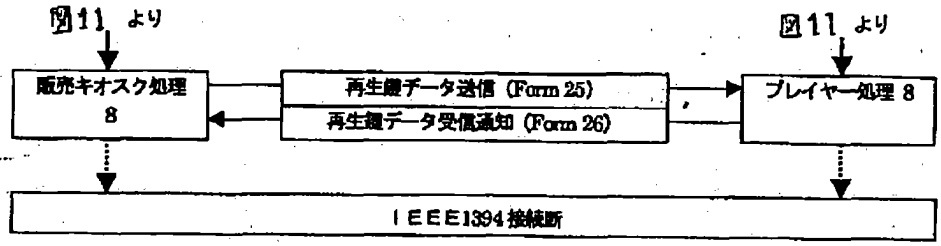
【図８】



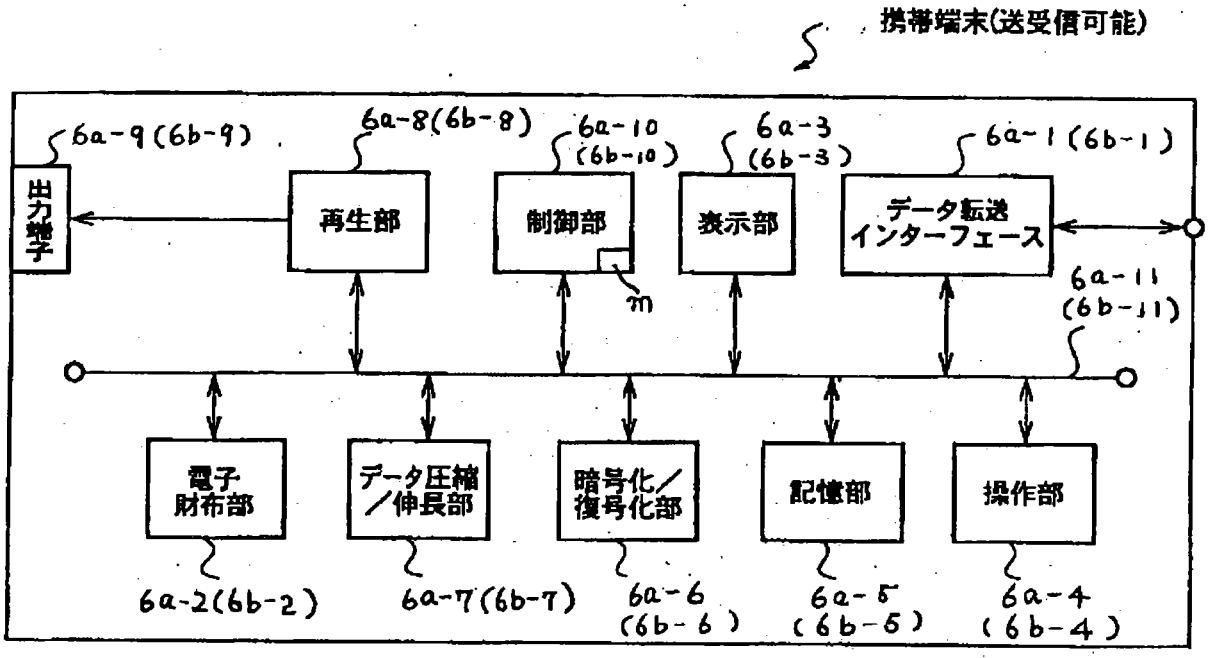
【図９】



【図１２】



【図１０】

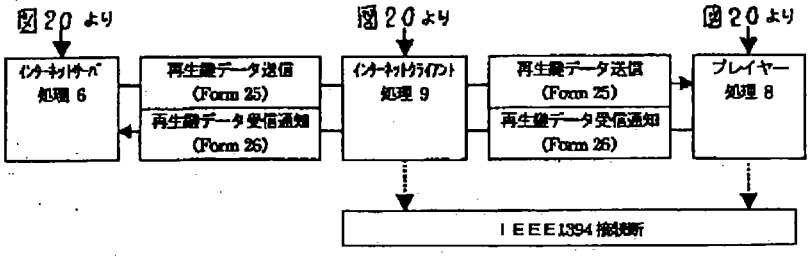


【図１４】

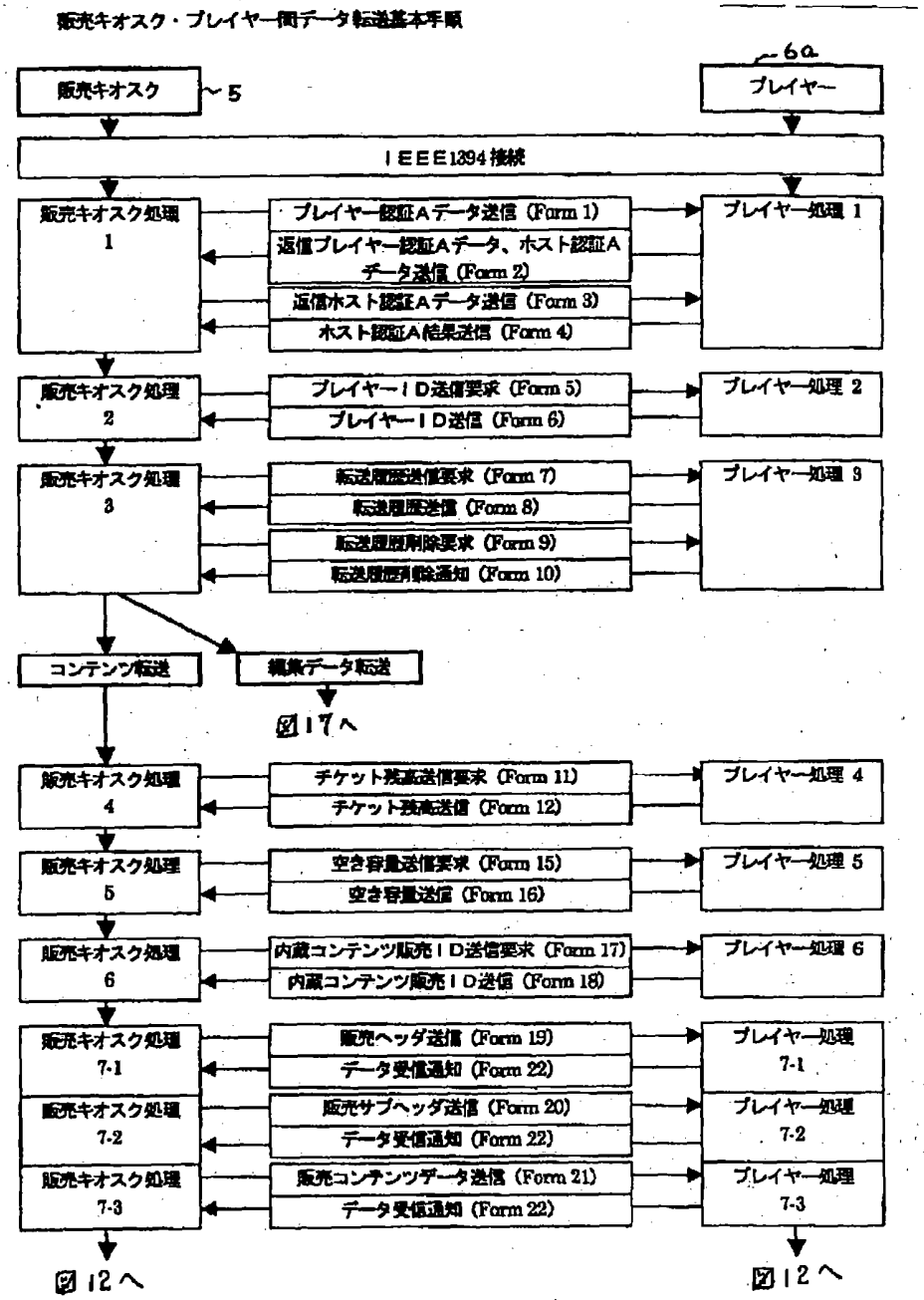
システム構成装置（発信元）のコード

00h	Reserved	08h	Reserved
01h	プレイヤー	09h	チケットサーバ
02h	販売キオスク	0Ah	販売オスク運用管理サーバ
03h	決済ボックス	0Bh	課金管理サーバ
04h	インターネットコンテンツ管理部	0Ch	インターネットクライアント
05h	インターネット決済管理部	0Dh	送信サーバ
06h	Reserved	0Eh	マスタリング／オーサリング
07h	Reserved	0Fh～FFh	Reserved

【図２１】



【図１１】

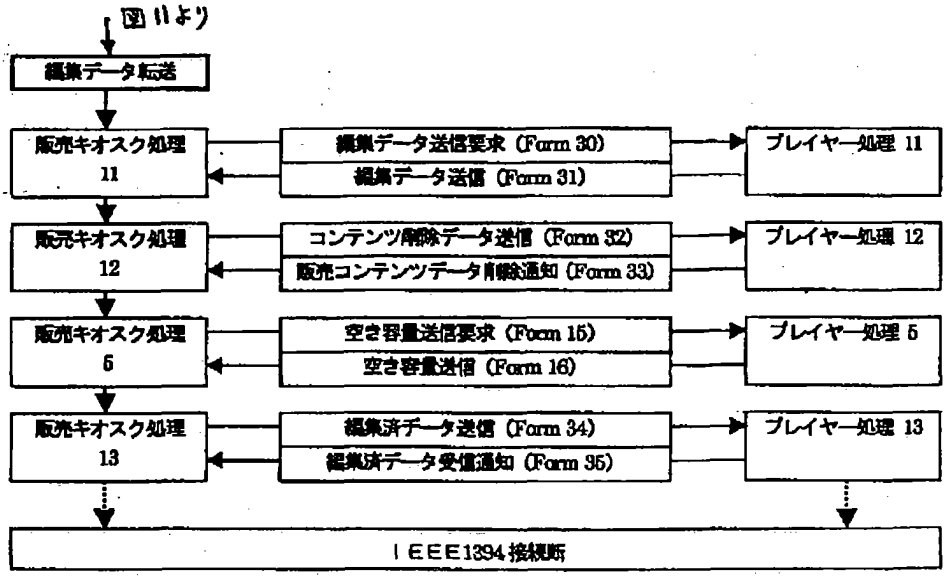

販売キオスク・プレイヤー間データ転送基本手順
販売キオスク
～5
～6a
プレイヤー
IEEE1394接続
販売キオスク処理 1
プレイヤー認証Aデータ送信 (Form 1)
返信プレイヤー認証Aデータ、ホスト認証Aデータ送信 (Form 2)
返信ホスト認証Aデータ送信 (Form 3)
ホスト認証A結果送信 (Form 4)
プレイヤー処理 1
販売キオスク処理 2
プレイヤーID送信要求 (Form 5)
プレイヤーID送信 (Form 6)
プレイヤー処理 2
販売キオスク処理 3
転送履歴送信要求 (Form 7)
転送履歴送信 (Form 8)
転送履歴削除要求 (Form 9)
転送履歴削除通知 (Form 10)
プレイヤー処理 3
コンテンツ転送
編集データ転送
図17へ
販売キオスク処理 4
チケット残高送信要求 (Form 11)
チケット残高送信 (Form 12)
プレイヤー処理 4
販売キオスク処理 5
空き容量送信要求 (Form 15)
空き容量送信 (Form 16)
プレイヤー処理 5
販売キオスク処理 6
内蔵コンテンツ販売ID送信要求 (Form 17)
内蔵コンテンツ販売ID送信 (Form 18)
プレイヤー処理 6
販売キオスク処理 7-1
販売ヘッダ送信 (Form 19)
データ受信通知 (Form 22)
プレイヤー処理 7-1
販売キオスク処理 7-2
販売サブヘッダ送信 (Form 20)
データ受信通知 (Form 22)
プレイヤー処理 7-2
販売キオスク処理 7-3
販売コンテンツデータ送信 (Form 21)
データ受信通知 (Form 22)
プレイヤー処理 7-3
図12へ
図12へ

【図１５】

コマンド (1/2)

00h～0Fh	Reserved
10h	プレイヤー認証Aデータ送信
11h	返信ホスト認証Aデータ送信
12h	プレイヤーＩＤ送信要求
13h	転送履歴送信要求
14h	転送履歴削除要求
15h	チケット残高送信要求
16h	チケット発行終了通知
17h	Reserved
18h	Reserved
19h	空き容量送信要求
1Ah	内蔵コンテンツ販売ＩＤ送信要求
1Bh	販売ヘッダ送信
1Ch	販売サブヘッダ送信
1Dh	販売コンテンツデータ送信
1Eh	Reserved
1Fh	再生鍵データ送信
20h	返信プレイヤー認証Aデータ、ホスト認証Aデータ送信
21h	ホスト認証A結果送信
22h	プレイヤーＩＤ送信
23h	転送履歴送信
24h	転送履歴削除通知
25h	チケット残高送信
26h	チケット発行受信通知
27h	Reserved
28h	Reserved
29h	空き容量送信
2Ah	内蔵コンテンツ販売ＩＤ送信

【図１７】

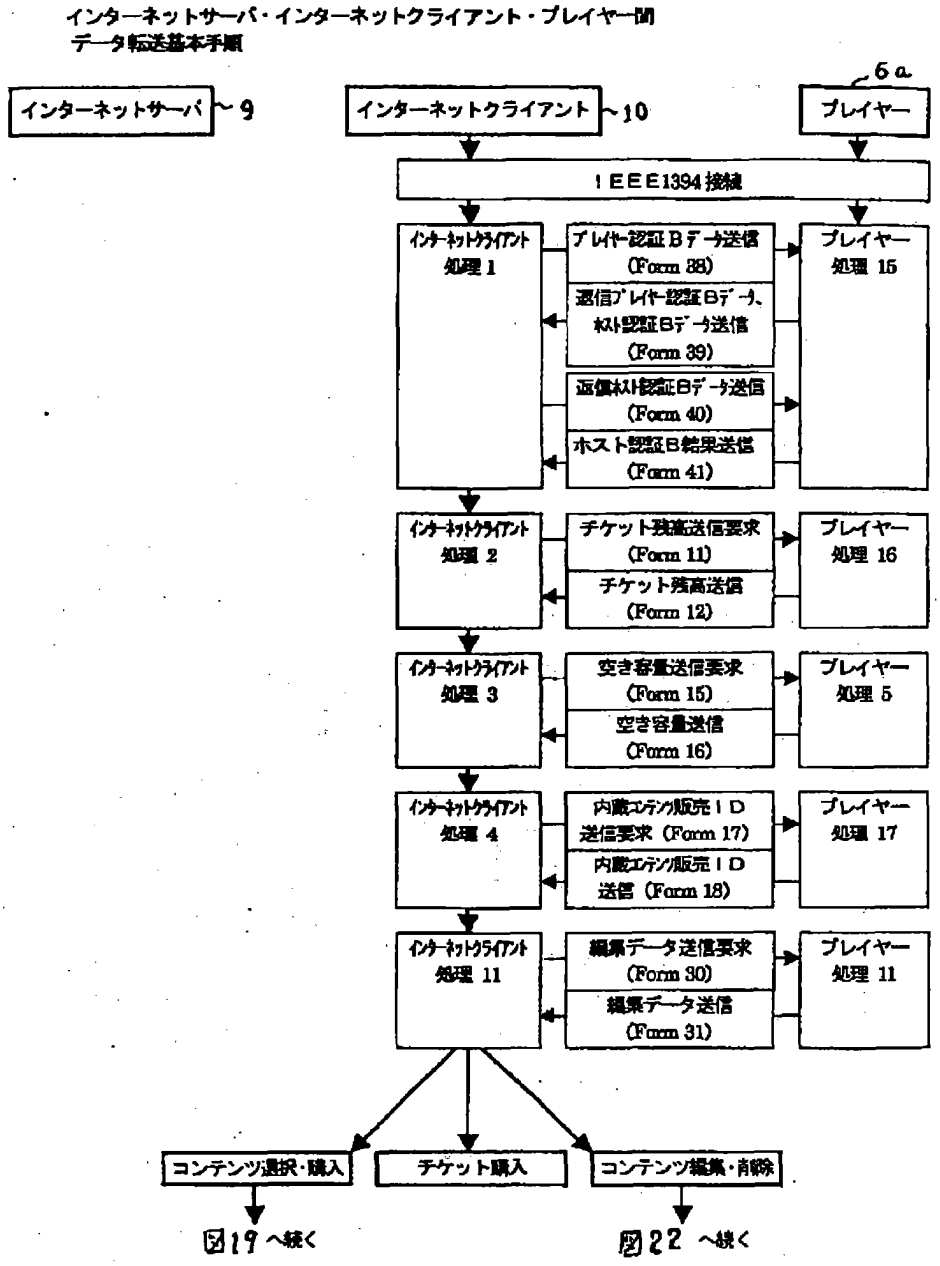


【図１６】

コマンド(2/2)

2Bh	Reserved
2Ch	Reserved
2Dh	再生鍵データ受信通知
2Eh	プレイヤー認証Bデータ送信
2Fh	返信ホスト認証Bデータ送信
30h	編集データ送信要求
31h	コンテンツ削除データ送信
32h	編集済データ送信
33h	Reserved
34h	Reserved
35h	Reserved
36h	Reserved
37h	Reserved
38h	編集データ送信
39h	販売コンテンツデータ削除通知
3Ah	編集済データ受信通知
3Bh	Reserved
3Ch	Reserved
3Dh	Reserved
3Eh	返信プレイヤー認証Bデータ、ホスト認証Bデータ送信
3Fh	ホスト認証B結果送信
40h～EFh	Reserved
F0h	Reserved
F1h	データ受信通知
F2h	コマンド受信通知
F3h	コマンド再送信要求
F4h	待機コマンド送信
F5h	Reserved
F6h	Reserved
F7h	Reserved
F8h	Reserved
F9h	Reserved
FAh	電子チケット転送
FBh	Reserved
FCh	Reserved
FDh	Reserved
FEh	Reserved
FFh	中止コマンド送信

【図１８】


インターネットサーバ・インターネットクライアント・プレイヤー間
データ転送基本手順
インターネットサーバ
9
インターネットクライアント
10
プレイヤー
6a
IEEE1394接続
インターネットクライアント処理 1
プレイヤー認証Bデータ送信 (Form 38)
返信プレイヤー認証Bデータ、ホスト認証Bデータ送信 (Form 39)
返信ホスト認証Bデータ送信 (Form 40)
ホスト認証B結果送信 (Form 41)
プレイヤー処理 15
インターネットクライアント処理 2
チケット残高送信要求 (Form 11)
チケット残高送信 (Form 12)
プレイヤー処理 16
インターネットクライアント処理 3
空き容量送信要求 (Form 15)
空き容量送信 (Form 16)
プレイヤー処理 5
インターネットクライアント処理 4
内蔵コンテンツ販売ＩＤ送信要求 (Form 17)
内蔵コンテンツ販売ＩＤ送信 (Form 18)
プレイヤー処理 17
インターネットクライアント処理 11
編集データ送信要求 (Form 30)
編集データ送信 (Form 31)
プレイヤー処理 11
コンテンツ選択・購入
チケット購入
コンテンツ編集・削除
図19へ続く
図22へ続く

【図１９】

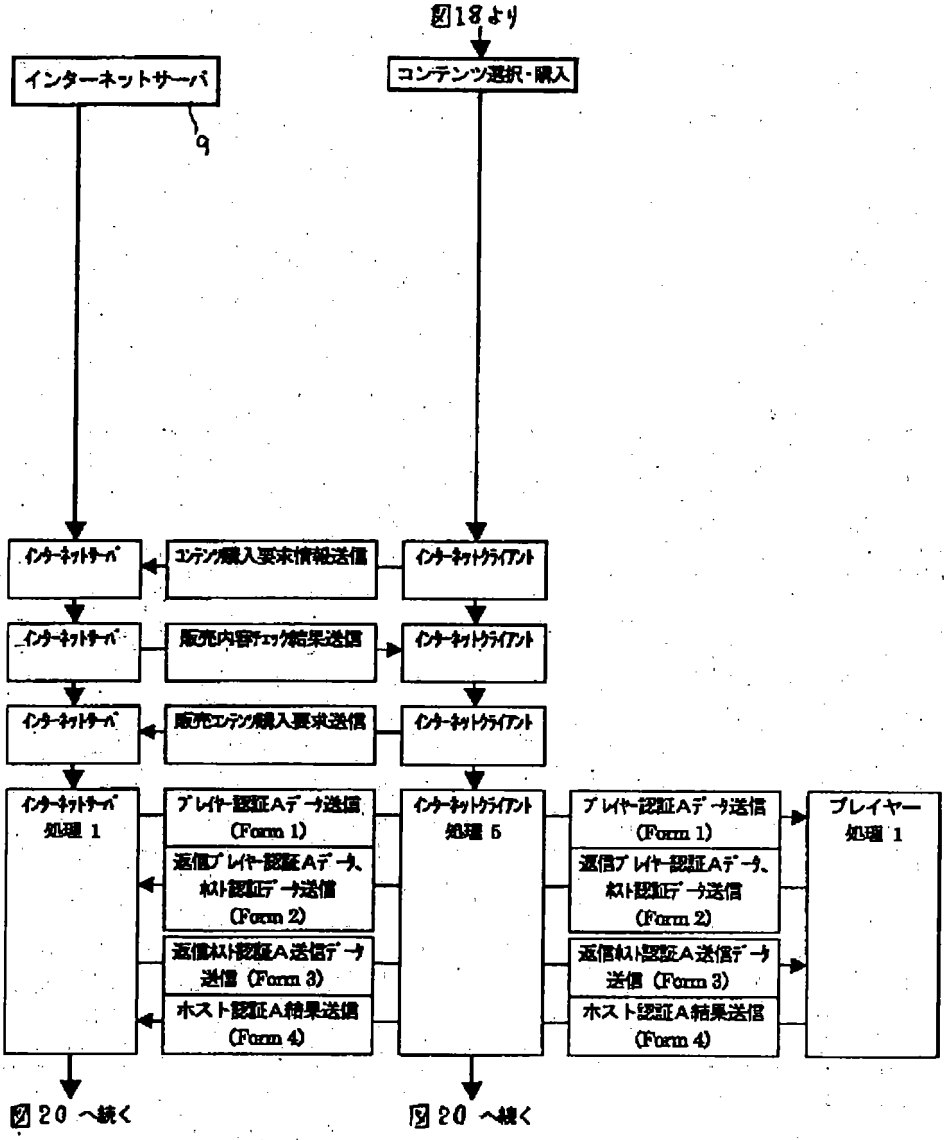


図18より
インターネットサーバ
9
コンテンツ選択・購入
インターネットサーバ
コンテンツ購入要求情報送信
インターネットクライアント
インターネットサーバ
販売内容チェック結果送信
インターネットクライアント
インターネットサーバ
販売コンテンツ購入要求送信
インターネットクライアント
インターネットサーバ
処理 1
プレイヤー認証Aデータ送信
(Form 1)
返信プレイヤー認証Aデータ、
ホスト認証データ送信
(Form 2)
返信ホスト認証A送信データ
送信 (Form 3)
ホスト認証A結果送信
(Form 4)
インターネットクライアント
処理 5
プレイヤー認証Aデータ送信
(Form 1)
返信プレイヤー認証Aデータ、
ホスト認証データ送信
(Form 2)
返信ホスト認証A送信データ
送信 (Form 3)
ホスト認証A結果送信
(Form 4)
プレイヤー
処理 1
図20へ続く
図20へ続く

【図２９】

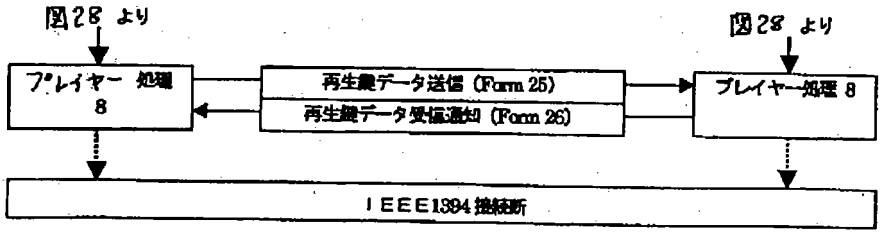


図28より
プレイヤー 処理
8
再生鍵データ送信 (Form 25)
再生鍵データ受信通知 (Form 26)
図28より
プレイヤー処理 8
IEEE1394接続断

【図２０】

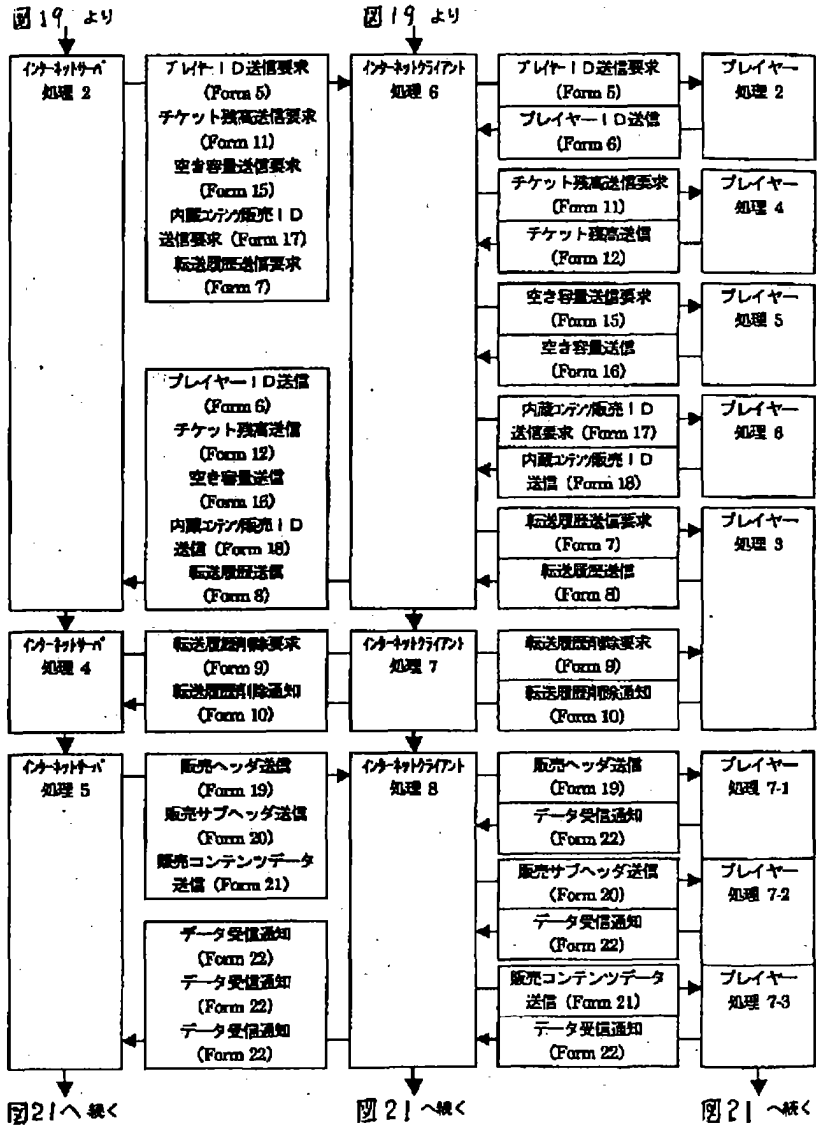
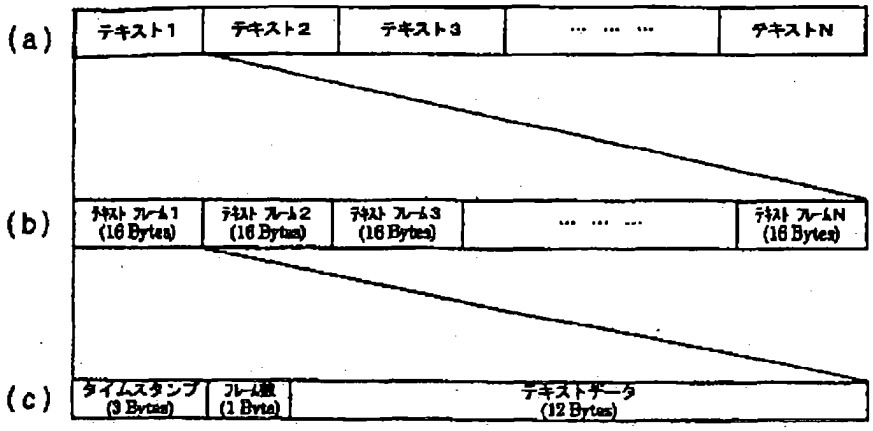


図19 より
図19 より
インターネットサーバ 処理 2
プレイヤーID送信要求 (Form 5)
チケット残高送信要求 (Form 11)
空き容量送信要求 (Form 15)
内蔵コンテンツ販売ID 送信要求 (Form 17)
転送履歴送信要求 (Form 7)
プレイヤーID送信 (Form 6)
チケット残高送信 (Form 12)
空き容量送信 (Form 16)
内蔵コンテンツ販売ID 送信 (Form 18)
転送履歴送信 (Form 8)
インターネットクライアント 処理 6
プレイヤーID送信要求 (Form 5)
プレイヤーID送信 (Form 6)
チケット残高送信要求 (Form 11)
チケット残高送信 (Form 12)
空き容量送信要求 (Form 15)
空き容量送信 (Form 16)
内蔵コンテンツ販売ID 送信要求 (Form 17)
内蔵コンテンツ販売ID 送信 (Form 18)
転送履歴送信要求 (Form 7)
転送履歴送信 (Form 8)
プレイヤー 処理 2
プレイヤー 処理 4
プレイヤー 処理 5
プレイヤー 処理 6
プレイヤー 処理 3
インターネットサーバ 処理 4
転送履歴削除要求 (Form 9)
転送履歴削除通知 (Form 10)
インターネットクライアント 処理 7
転送履歴削除要求 (Form 9)
転送履歴削除通知 (Form 10)
インターネットサーバ 処理 5
販売ヘッダ送信 (Form 19)
販売サブヘッダ送信 (Form 20)
販売コンテンツデータ送信 (Form 21)
データ受信通知 (Form 22)
データ受信通知 (Form 22)
データ受信通知 (Form 22)
インターネットクライアント 処理 8
販売ヘッダ送信 (Form 19)
データ受信通知 (Form 22)
販売サブヘッダ送信 (Form 20)
データ受信通知 (Form 22)
販売コンテンツデータ送信 (Form 21)
データ受信通知 (Form 22)
プレイヤー 処理 7-1
プレイヤー 処理 7-2
プレイヤー 処理 7-3
図21へ続く
図21へ続く
図21へ続く

【図３０】


(a)
テキスト1
テキスト2
テキスト3
… … …
テキストN
(b)
テキスト フレーム1 (16 Bytes)
テキスト フレーム2 (16 Bytes)
テキスト フレーム3 (16 Bytes)
… … …
テキスト フレームN (16 Bytes)
(c)
タイムスタンプ (3 Bytes)
フレーム数 (1 Byte)
テキストデータ (12 Bytes)

【図２２】

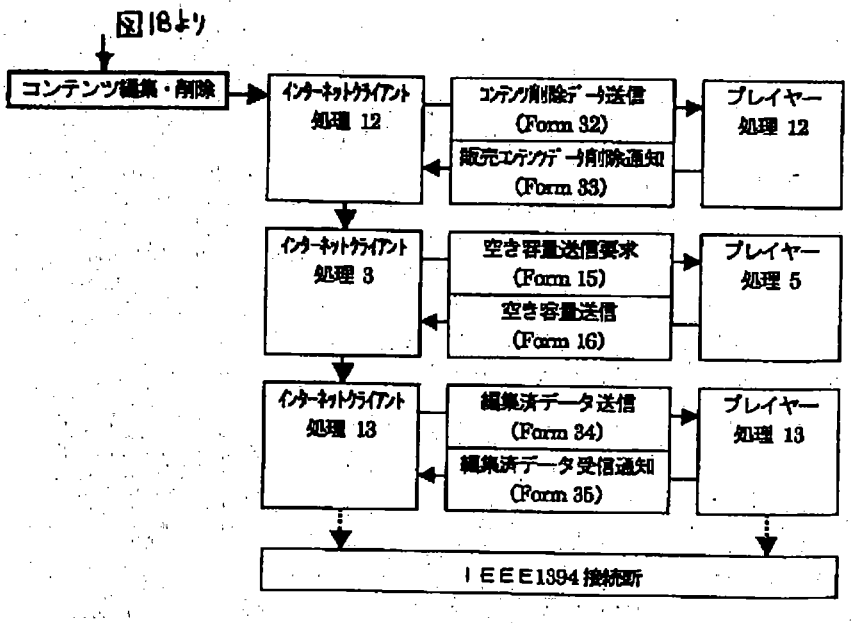
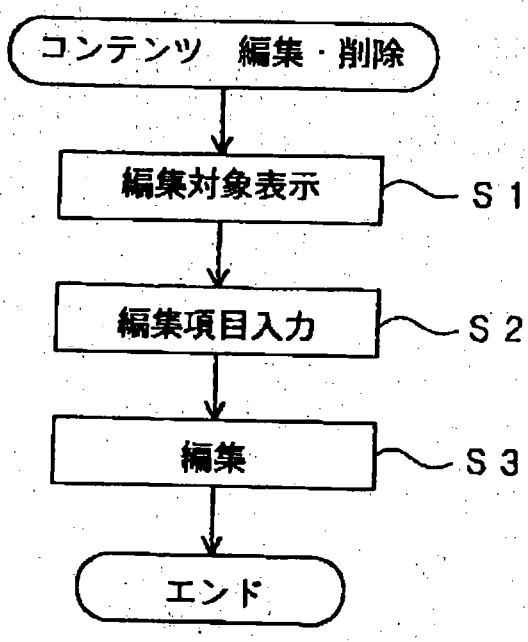


図18より
コンテンツ編集・削除
インターネットクライアント処理 12
コンテンツ削除データ送信 (Form 32)
販売コンテンツデータ削除通知 (Form 33)
プレイヤー処理 12
インターネットクライアント処理 3
空き容量送信要求 (Form 15)
空き容量送信 (Form 16)
プレイヤー処理 5
インターネットクライアント処理 13
編集済データ送信 (Form 34)
編集済データ受信通知 (Form 35)
プレイヤー処理 13
IEEE1394接続断

【図２３】


コンテンツ　編集・削除
編集対象表示
S 1
編集項目入力
S 2
編集
S 3
エンド

【図２４】

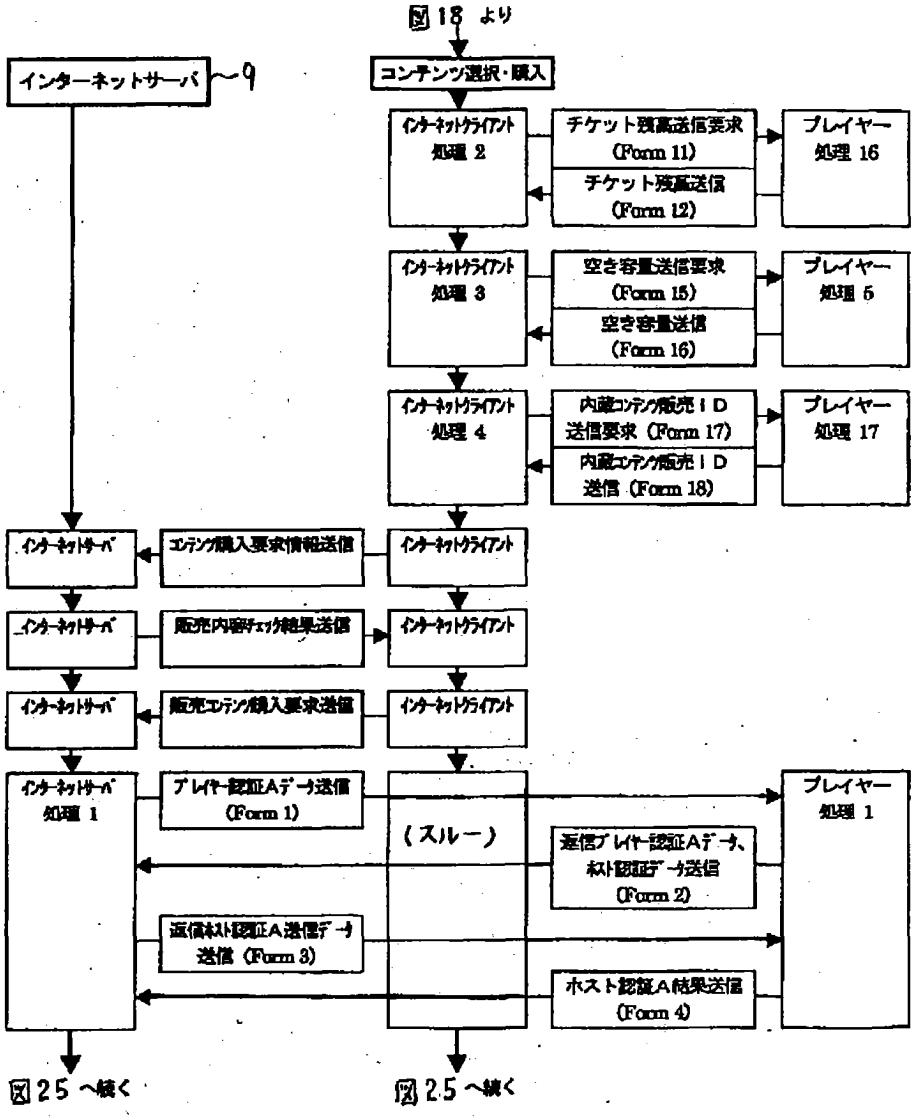


図18 より
インターネットサーバ
9
コンテンツ選択・購入
インターネットクライアント 処理 2
チケット残高送信要求 (Form 11)
チケット残高送信 (Form 12)
プレイヤー 処理 16
インターネットクライアント 処理 3
空き容量送信要求 (Form 15)
空き容量送信 (Form 16)
プレイヤー 処理 5
インターネットクライアント 処理 4
内蔵コンテンツ販売ＩＤ送信要求 (Form 17)
内蔵コンテンツ販売ＩＤ送信 (Form 18)
プレイヤー 処理 17
インターネットサーバ
コンテンツ購入要求情報送信
インターネットクライアント
インターネットサーバ
販売内容チェック結果送信
インターネットクライアント
インターネットサーバ
販売コンテンツ購入要求送信
インターネットクライアント
インターネットサーバ 処理 1
プレイヤー認証Aデータ送信 (Form 1)
（スルー）
返信プレイヤー認証Aデータ、ホスト認証データ送信 (Form 2)
プレイヤー 処理 1
返信ホスト認証A送信データ送信 (Form 3)
ホスト認証A結果送信 (Form 4)
図25 へ続く
図25 へ続く

【図２５】

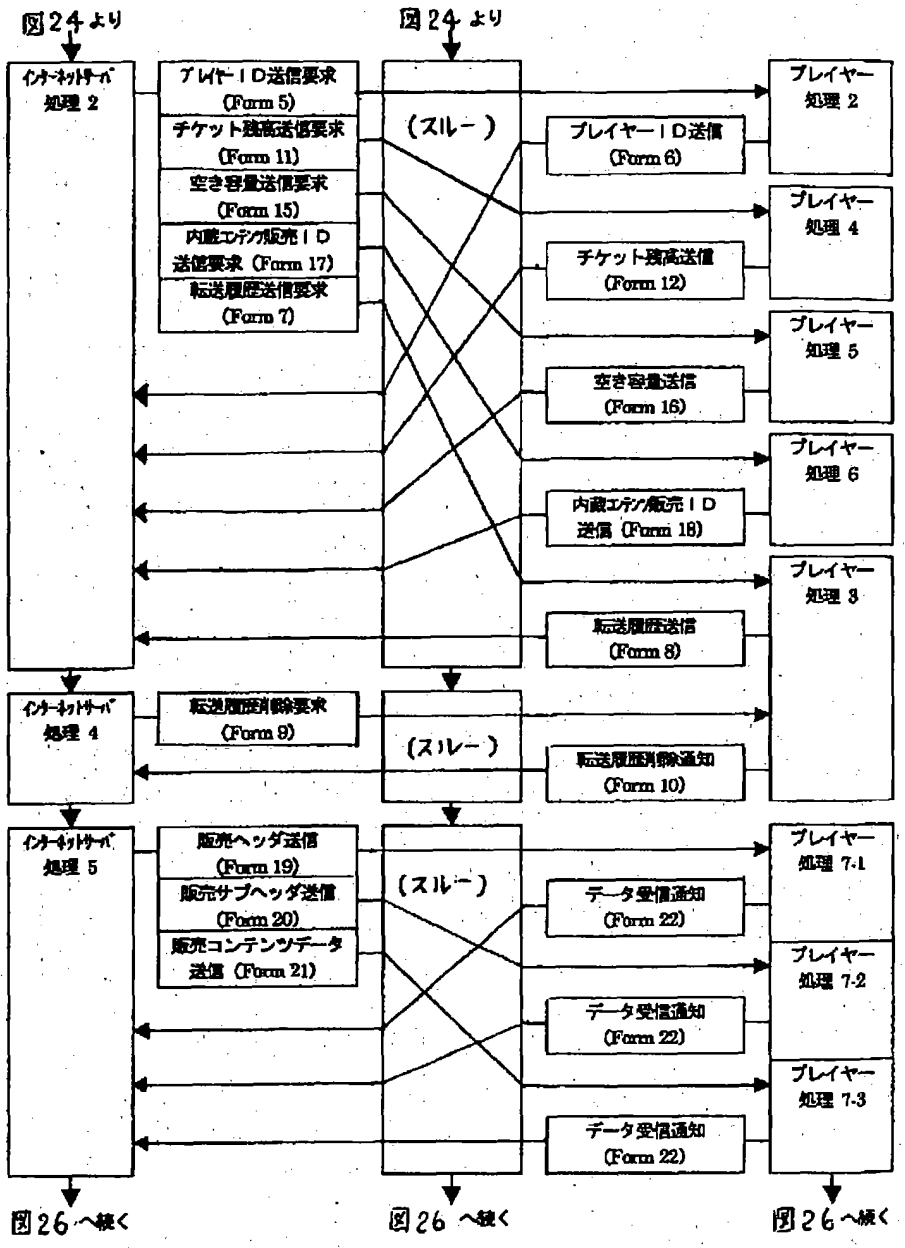


図24より
図24より
インターネットサーバ処理 2
プレイヤーＩＤ送信要求 (Form 5)
チケット残高送信要求 (Form 11)
空き容量送信要求 (Form 15)
内蔵コンテンツ販売ＩＤ送信要求 (Form 17)
転送履歴送信要求 (Form 7)
(スルー)
プレイヤーＩＤ送信 (Form 6)
チケット残高送信 (Form 12)
空き容量送信 (Form 16)
内蔵コンテンツ販売ＩＤ送信 (Form 18)
転送履歴送信 (Form 8)
プレイヤー処理 2
プレイヤー処理 4
プレイヤー処理 5
プレイヤー処理 6
プレイヤー処理 3
インターネットサーバ処理 4
転送履歴削除要求 (Form 9)
(スルー)
転送履歴削除通知 (Form 10)
インターネットサーバ処理 5
販売ヘッダ送信 (Form 19)
販売サブヘッダ送信 (Form 20)
販売コンテンツデータ送信 (Form 21)
(スルー)
データ受信通知 (Form 22)
データ受信通知 (Form 22)
データ受信通知 (Form 22)
プレイヤー処理 7-1
プレイヤー処理 7-2
プレイヤー処理 7-3
図26へ続く
図26へ続く
図26へ続く

【図２６】

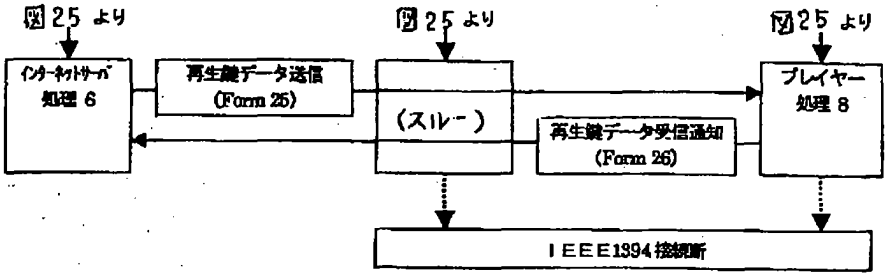
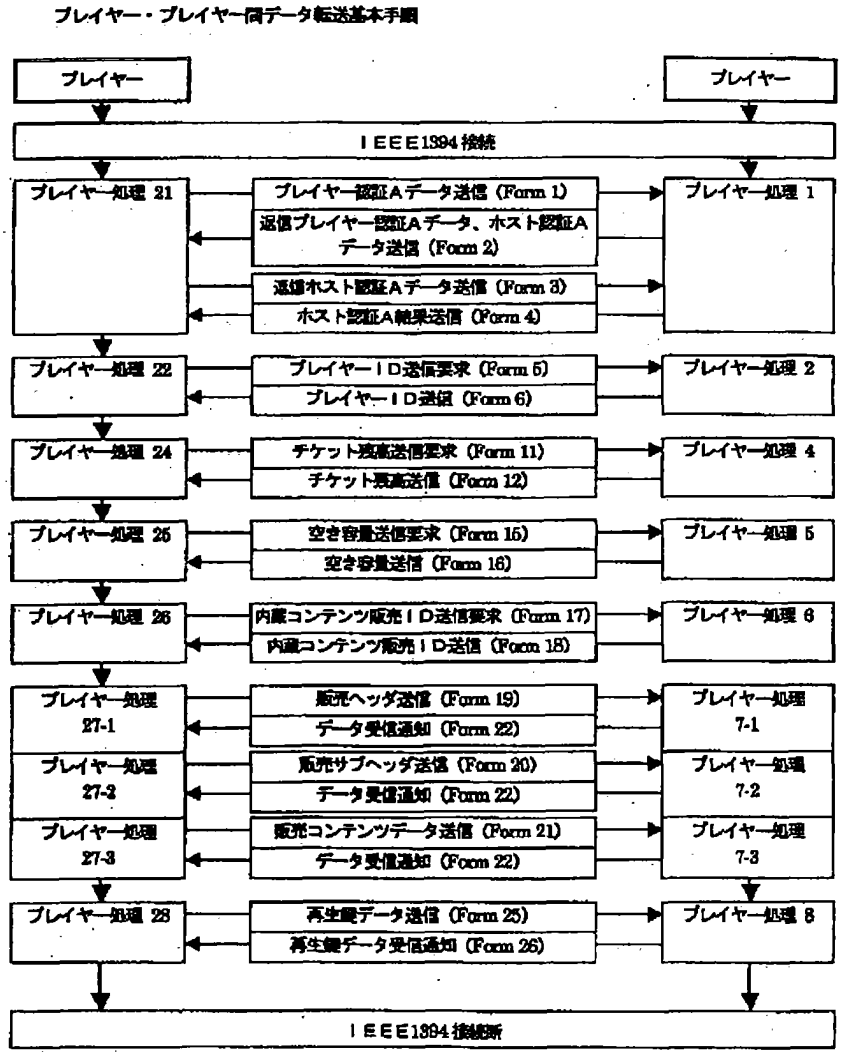
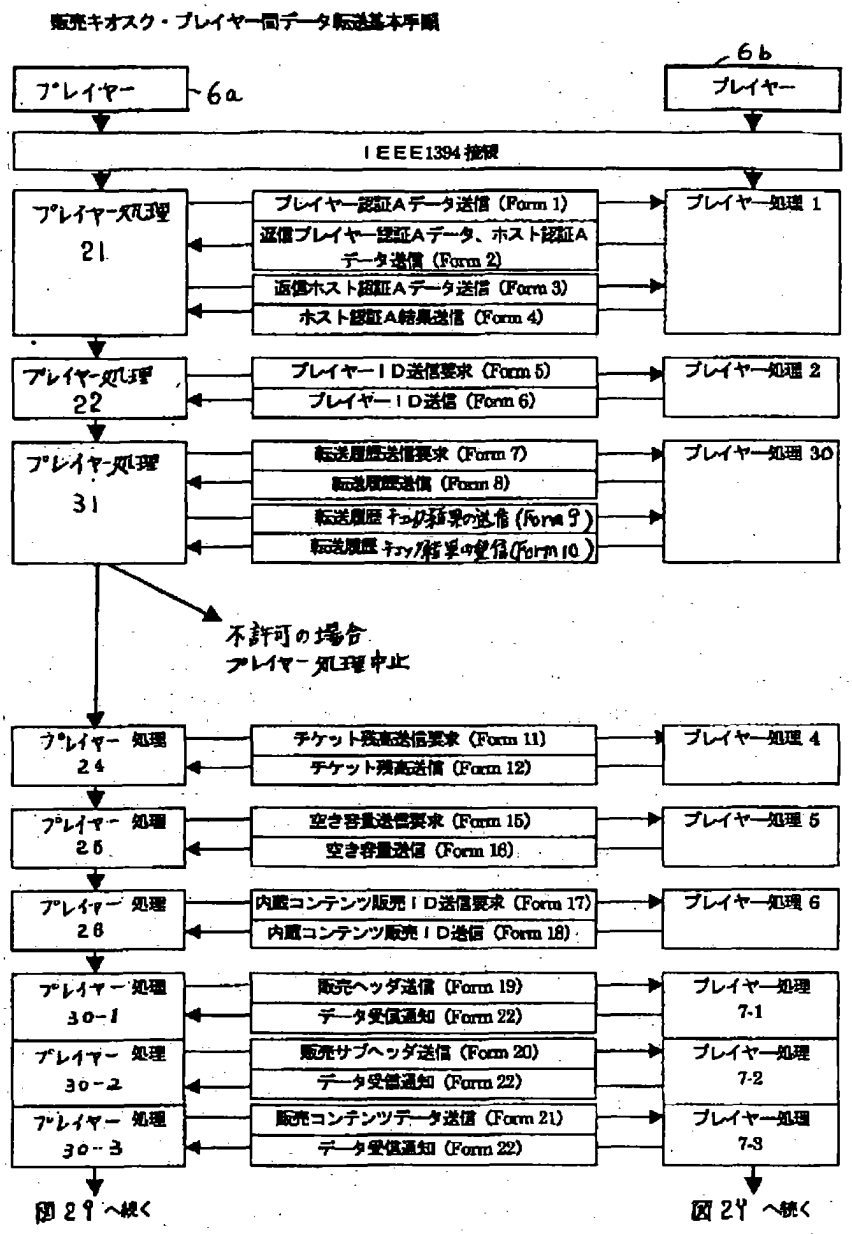


図25 より
図25 より
図25 より
インターネットサーバ処理 6
再生鍵データ送信 (Form 25)
(スルー)
再生鍵データ受信通知 (Form 26)
プレイヤー処理 8
IEEE1394 接続断

【図２７】


プレイヤー・プレイヤー間データ転送基本手順
プレイヤー
プレイヤー
IEEE1394 接続
プレイヤー処理 21
プレイヤー認証Aデータ送信 (Form 1)
返信プレイヤー認証Aデータ、ホスト認証Aデータ送信 (Form 2)
返信ホスト認証Aデータ送信 (Form 3)
ホスト認証A結果送信 (Form 4)
プレイヤー処理 1
プレイヤー処理 22
プレイヤーID送信要求 (Form 5)
プレイヤーID送信 (Form 6)
プレイヤー処理 2
プレイヤー処理 24
チケット残高送信要求 (Form 11)
チケット残高送信 (Form 12)
プレイヤー処理 4
プレイヤー処理 25
空き容量送信要求 (Form 15)
空き容量送信 (Form 16)
プレイヤー処理 5
プレイヤー処理 26
内蔵コンテンツ販売ID送信要求 (Form 17)
内蔵コンテンツ販売ID送信 (Form 18)
プレイヤー処理 6
プレイヤー処理 27-1
販売ヘッダ送信 (Form 19)
データ受信通知 (Form 22)
プレイヤー処理 7-1
プレイヤー処理 27-2
販売サブヘッダ送信 (Form 20)
データ受信通知 (Form 22)
プレイヤー処理 7-2
プレイヤー処理 27-3
販売コンテンツデータ送信 (Form 21)
データ受信通知 (Form 22)
プレイヤー処理 7-3
プレイヤー処理 28
再生鍵データ送信 (Form 25)
再生鍵データ受信通知 (Form 26)
プレイヤー処理 8
IEEE1394 接続断

【図２８】



フロントページの続き

(51)Int.Cl.7	識別記号	FI		テーマコード(参考)
G10L 19/02		G10L 7/04		G 5J104
19/00			9/00	N
11/00				E
H04L 9/20			9/18	M
H04N 7/167		H04L 9/00		653

H04N 7/167 Z

Fターム(参考) 5B017 AA06 BA05 BA07 BB03 BB10
CA07 CA11 CA16
5B082 AA11 CA07 CA08 EA01 EA12
GA01 GA02 GC05
5B085 AE06 AE13 AE29
5C064 BA07 BB02 CA16 CB01 CC04
5D045 DA20
5J104 AA01 AA35 JA04 JA13 NA02
PA07